Deloitte.

The Risk Intelligent chief compliance officer

Champion of Risk Intelligent compliance

Risk Intelligence series

Contents

3 Preface

4 Foreword: Who should read this publication?

5 Executive summary

6 The role that everyone loves to hate?

9 The Risk Intelligent CCO's defining characteristic

11 The building blocks of Risk Intelligent compliance

17 Toward Risk Intelligent compliance

21 Epilogue: The value of insight and control

22 Appendix: A portrait of compliance in the Risk Intelligent Enterprise

23 Endnotes

24 Nine fundamental principles of a Risk Intelligence program

25 Contact us

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.

Foreword: Who should read this publication?

The Risk Intelligent Chief Compliance Officer explores ideas that should interest many readers besides the eponymous compliance executive. The risk-based approach to compliance it describes — "Risk Intelligent compliance" — depends just as much, if not more, on broad organizational engagement as on the Chief Compliance Officer's (CCO's) leadership. Accordingly, we offer this publication as a resource to professionals in a variety of roles, including:

- **CCOs** seeking to strengthen their companies' compliance efforts
- **Other C-suite executives** interested in increasing compliance's contribution to enterprise value
- **Boards of directors** who want to understand what they should expect from an effective compliance program
- **"De facto CCOs"** who, although not known by the title of CCO, are nonetheless responsible for overseeing compliance across multiple organizational areas
- **Compliance, internal audit, legal, human resources, internal control, and corporate security professionals** wishing to broaden their understanding of compliance's role in today's corporate environment

Executive summary

How to read this paper in five minutes or less
A box like this one at the start of each chapter briefly summarizes the chapter's contents.

Compliance is a fundamental enterprise risk that companies have faced since long before enterprise risk management (ERM) became a fixture of modern business. Yet compliance may still be the risk that commands the least attention from corporate leadership. Other types of risk — strategic, operational, financial — often receive a great deal of focus as risks a company may need to take to advance its strategic plan. Compliance, in contrast, is too frequently seen as an imposition from outside, a necessary evil, a risk without a corresponding reward.

We invite CCOs to turn this view of compliance on its head through the practice of Risk Intelligent compliance. With Risk Intelligent compliance, leaders accept compliance risk as a fact of life — and charge the CCO with keeping that risk below the "comfort level" set by company leaders and owners. While compliance failures are never acceptable, leaders may be willing to accept substantial inherent compliance risk if the prospective gains seem worth it and if they believe the company capable of keeping residual compliance risk within tolerance.

Risk Intelligent compliance is distinguished by three core attributes:

- **Ongoing alignment of compliance investments and activities with business priorities.** To this end, the Risk Intelligent CCO applies an ERM-aligned compliance risk management framework that evaluates each compliance risk's business significance in the context of the company's "macro" risks and goals.
- **Widespread recognition of compliance's potential impact on multiple dimensions of enterprise value.** Through influence and advocacy, the Risk Intelligent CCO helps stakeholders appreciate the far-reaching effects that compliance incidents can have on reputation, strategy, operations, and finance.
- **The use of the company's compliance strengths to pursue "upside" business value.** The Risk Intelligent CCO promotes a healthy respect for the extent to which effective compliance underlies the ability to execute strategic initiatives, and actively participates in strategic planning to identify ways to leverage the company's compliance capabilities to pursue competitive advantage.

As champion of Risk Intelligent compliance, the Risk Intelligent CCO will embrace the challenge of engaging stakeholders across the enterprise in its pursuit. ERM leadership involvement is critical, as is the support of the CEO and the board of directors. To improve compliance efficiency and effectiveness, the CCO may consider investing in more effective compliance technology and working with other stakeholders, especially internal audit, to reduce duplication of effort. Finally, the CCO can help establish a culture of compliance with a change management effort that buttresses communications and training with a performance management and compensation structure that ties appropriate individuals' rewards to important compliance objectives.

With regulations and reputational concerns pushing compliance leaders to the top levels of management, the time is ripe for them to act. For the Risk Intelligent CCO, the pursuit of Risk Intelligent compliance can be an opportunity to put compliance on a value-driven footing that can transform compliance, long seen as a chore, into a valued and valuable business asset.

The role that everyone loves to hate?

Mounting compliance obligations and heightened regulatory and legal oversight have made corporate compliance a daunting and growing challenge. Fortunately, today's CCOs are in a position to do something about it. With regulations and reputational concerns pushing compliance leaders to the top levels of management, CCOs have the opportunity to transform compliance, long viewed as a chore, into a valued and valuable business asset.

Naysayer. Deal-killer. "Dr. No." Many CCOs may recognize these as some of the more printable epithets aimed at them, jokingly or otherwise, by people throughout "the business." Most, to their credit, know better than to take it personally. They know that compliance can be a hassle even when people agree with the regulations in question. They understand that frustrations can run even higher among those who see compliance as a hindrance. Many may accept a certain amount of invective as part of the job. After all, it's an inevitable part of the territory of leading a function whose sole *raison d'être* is to make everybody toe the line.

Or does it? Consider a different view of the CCO role, and that of compliance in general. One where the business values compliance because they appreciate compliance's value to the business. One where compliance professionals spend less time saying "no" and more time helping people understand when to say "no" — or "yes" — for themselves. One where compliance not only helps keep the business out of trouble, but actively helps it to grow and thrive.

No, we're not dreaming. Though this vision may still be a far cry from how most companies see compliance, CCOs today are better placed to make meaningful progress toward it than at any time in the past. As the compliance function's leader, the CCO can align its oversight efforts with ERM and business goals. As the steward of enterprise-wide compliance, the CCO can help educate people about why compliance matters and how they can effectively support it. And as a senior executive with board-level visibility, the CCO can help the enterprise use its strengths in compliance to seek competitive advantage.

It may seem a tall order, especially considering how much most CCOs' workloads and responsibilities have grown over the past decade. Burgeoning compliance obligations and heightened expectations around transparency have increased compliance's operational challenges, while stricter enforcement efforts and relentless public scrutiny have magnified its potential business impact. On the other hand, the same forces that have multiplied the challenges and raised the stakes have also made compliance a board-level concern, given compliance a champion in the C-suite, and even sparked a growing financial commitment to compliance.[1] The CCO's cup may not runneth over, but the glass might now at least be half full.

With the environment priming companies to be receptive, today's CCOs have an unparalleled opportunity to help compliance become the smart business investment that it could and should be. More than that, they have an obligation to do so. And it doesn't have to cause CCOs more work or more stress, at least not in the long run. In fact, it may even help them make headway on both workload and worry by allowing them to prioritize their efforts on grounds that the rest of the organization supports.

The approach described here shows how applying the general principles of Risk Intelligence to the specific challenges of compliance can bring about a sea change in compliance's relationship with, and contribution to, the business. It's a blueprint for orienting an enterprise to ways of thinking and acting that can give leaders greater control over compliance risk exposures while holding compliance cost and effort to sustainable levels. We'll explore ways that CCOs can help begin the transformation and accelerate its progress, both directly through the compliance function and indirectly by driving ownership and accountability among stakeholders throughout the organization. The goal: to help the enterprise, through Risk Intelligent compliance, harness compliance as an engine for business value.

I'm laughing so hard, I can't stop crying

With their rise in corporate status seemingly matched only by the growth in their burdens, many CCOs may feel like they're trapped in a bad comedy routine. Consider:

Fortunately…	Unfortunately…
More CCOs every year are getting budget and staffing increases. According to a 2011 survey, "The Economy, Compliance, and Ethics," the proportion of compliance officers receiving budget increases has risen every year since 2009, as has the proportion able to add compliance staff.[2]	**It's still not enough.** Only 27 percent of the compliance officers in a separate 2011 survey, "Stress, Compliance, and Ethics," thought that their current budgets were enough to support their organizations' compliance programs. Fully 29 percent said that they had "nowhere near enough" budget.[3]
At most companies, management has a generally positive view of compliance. Most of the compliance officers in the "Economy, Compliance, and Ethics" survey said that management saw compliance as a somewhat or very positive asset in helping their organizations address current economic conditions.	**The positive view hasn't trickled down to the rank and file.** Fifty-eight percent of the compliance officers in the "Stress, Compliance, and Ethics" survey felt that they were in an "adversarial situation or isolated from" colleagues in other departments.
Thanks to regulators and other authorities, many companies now have a CCO or equivalent senior-level compliance executive. For instance, the U.S. Department of Justice and other federal regulators, in corporate consent decrees and corporate integrity agreements, routinely require companies to appoint officer-level CCOs who are not subordinate to the CFO or General Counsel and who have direct access to the company's board of directors.	**Thanks to regulators and other authorities, companies face a growing number of compliance obligations, and there's no sign of the pace slowing down.** "Keeping up with new laws and regulations" was the number-one stressor identified by compliance officers in the "Stress, Compliance, and Ethics" survey.
Boards now must be involved in compliance. A landmark 1996 decision by the Delaware Chancery Court effectively requires U.S. boards to be knowledgeable about the content and operation of a company's compliance program. Recent amendments to the U.S. Federal Sentencing Guidelines, effective since November 2010, further raised the stakes by expressly recommending that the top compliance executive at publicly traded U.S. companies have "direct reporting obligations" to the board or a subgroup thereof.[4]	**Most boards think compliance takes too much time as it is.** Sixty-four percent of public-company board members in a 2011 survey said that they wanted to spend less time on compliance and regulatory issues. (On the plus side, 55 percent also said that they wanted to spend more time on risk management — of which compliance is an important part.)[5]
CCOs may enjoy above-average job security. Despite the possibility of retaliatory firing,[6] 77 percent of the compliance officers in the "Economy, Compliance, and Ethics" survey felt that their jobs were at least as safe as those of others within their organizations. Fifty-two percent were "not at all concerned" about losing their jobs.	**Most CCOs find the job so stressful that they've considered quitting.** Sixty percent of the respondents to the "Stress, Compliance, and Ethics" survey admitted that job-related stress drove them to consider leaving their job over the last 12 months. Fifty-eight percent also reported that they "often" wake up in the middle of the night worrying about job-related stress.

Bigger challenges, higher stakes

Most readers probably don't need to be reminded of the factors in today's compliance environment that — literally — keep many CCOs awake at night. For those who want a refresher, here's a quick rundown:

- **Businesses are subject to more laws and regulations than ever, and the laws and regulations address a wider variety of issues.** At some companies, the sheer volume of compliance obligations can be a major obstacle to effective compliance execution and oversight. Additionally, new compliance requirements in previously unregulated areas can impose a steep learning curve on companies unfamiliar with the issues at hand as they race against the clock to understand the requirements and develop effective compliance approaches.
- **Companies are being held to higher standards of evidence of compliance.** Apart from their expectation that companies be compliant, authorities' standards for demonstrating compliance have become more stringent. A spreadsheet-based tracking and reporting process that might have passed muster 10 years ago could now invite, if not an actual sanction, a strong recommendation that the company invest in a more rigorous and controllable method of documentation. Speed of response is also an issue: Authorities expect businesses to be able to produce documented evidence of programmatic compliance at a moment's notice.
- **Compliance itself is now subject to compliance.** Regulators and standard-setting bodies have set requirements around the effectiveness of a company's compliance (and risk management) programs, adding a layer of compliance-focused obligations to many companies' business-focused obligations. The need for "compliance about compliance" not only adds to a company's total compliance-related workload, but also heightens the need for transparency into compliance controls, processes, and activities.
- **New whistleblower regulations may increase the chances of compliance failures being "caught."** The Dodd-Frank Act of 2010, for example, offers new incentives to whistleblowers who provide the U.S. Securities and Exchange Commission (SEC) with original information about securities law violations that results in an enforcement penalty of more than $1 million. Anonymous whistleblowers must be represented by counsel, which can invite further scrutiny and second-guessing.
- **Penalties for compliance failures have become more severe, putting executives and boards at greater personal risk.** Although corporate entities remain regulators' primary focus, authorities can still impose sanctions up to and including felony charges and possible prison terms for specific board members and business leaders.
- **Compliance has become a board-level concern.** Stock exchange listing requirements and regulatory mandates have made compliance a standing board responsibility. While this can work to a CCO's advantage, it also means that the company's compliance-related workload now includes the production of regular reports to the board; that investors are likely to be better informed about the company's compliance status; and that the CCO is now personally visible to the board and the public.
- **Investors, lenders, rating agencies, customers, suppliers, the media, and the general public care about compliance, and it's easy for them to stay informed about it.** Especially in areas that attract a great deal of media attention (such as lending practices, corruption, or social/environmental responsibility), compliance failures can compromise a company's reputation much more than when the only people who knew were the regulators. Moreover, some credit rating agencies and shareholder advocacy groups now offer ratings of U.S. public companies' corporate governance practices (including compliance practices), giving interested parties the opportunity to consider compliance and corporate governance alongside financial metrics in their decisions on whether to invest or do business with a company.

The Risk Intelligent CCO's defining characteristic

Compliance risk is an inevitable part of business. The Risk Intelligent CCO is responsible for managing that risk so as to keep it within the company's comfort zone ("tolerance"). To do this, he or she uses a Risk Intelligent compliance approach designed to give leaders a high level of insight into and control over the company's compliance obligations, risks, and controls, allowing them to align compliance efforts and investments with business priorities.

Leaders may be willing to accept substantial inherent compliance risk if the prospective gains seem worth it and if they believe that the company's compliance efforts can keep its residual compliance risk within tolerance. What they cannot accept, however, are known compliance failures. Simply put, if your business is out of compliance, you have the ethical obligation to bring it back into compliance.

The Risk Intelligent CCO understands that his or her job is to manage compliance risk, not to eliminate compliance failures. That, in a nutshell, is what gives CCOs the basis for architecting a Risk Intelligent compliance program that can help align a company's compliance efforts and investments with the pursuit of enterprise value.

A compliance failure can be defined as the state of being in violation of laws, regulations, company policies, or other applicable external or internal requirements. As a responsible corporate citizen, the Risk Intelligent Enterprise should view compliance failures as unacceptable — period. Whether reported or unreported, inadvertent or intentional, compliance failures should be promptly dealt with on two fronts: to redress the violation (for instance, by paying applicable fines or addressing personnel-related issues) and to determine if the company should remediate or enhance the internal control environment to reduce the risk of recurrence.[7]

Compliance risk, on the other hand, can be broadly defined as the possibility of experiencing adverse consequences as a result of a compliance incident.[8], [9] Like all risks, compliance risks can be understood both in terms of "inherent risk" — what would be the risk associated with a compliance incident if we were doing nothing to address it? — and "residual risk" — what, given the controls and procedures we currently have, is the risk we actually face?

The Risk Intelligent CCO is responsible for managing a company's residual compliance risk so that it remains below a specified upper limit, or "tolerance." The compliance risk tolerance, in turn, should be set by the CCO, senior management, and the board to reflect a reasonable and responsible comfort level with residual compliance risk.

Crucially, few if any leadership teams would set the compliance risk tolerance to zero. This isn't just because controls are imperfect, people are fallible, and processes and technology sometimes go wrong. It's because it's virtually impossible to conduct business at all without doing something subject to legal or regulatory oversight. Moreover — because controls are imperfect, people are fallible, and processes and technology sometimes go wrong — no control environment can guarantee 100 percent protection against compliance failures. And this means that the only way to completely eliminate residual compliance risk is to completely avoid all compliance obligations — in which case an organization might as well give up doing business altogether.

Depending on their attitudes toward risk, a company's leaders and owners may be willing to incur substantial inherent compliance risk if the potential returns seem worth it and if they believe the control environment capable of keeping residual compliance risk within tolerance. Furthermore, leaders can have a reasonable and responsible tolerance for residual compliance risk while still maintaining a zero-tolerance policy for known compliance failures. To use an everyday analogy, many people who run for fitness willingly tolerate a slightly higher risk of joint injury (relative to non-runners) as a fair trade for running's overall health benefits. That doesn't mean they ignore it if their knees start to hurt.

At a Risk Intelligent Enterprise, leaders accept inherent compliance risk as a fact of life, assume compliance obligations with a firm understanding of the risk-reward tradeoffs, and, for the compliance obligations they assume, invest in controls and other compliance mechanisms in the manner and degree needed — no more, no less — to keep residual compliance risk within tolerance. To do this effectively, leaders need a great deal of insight into and control over compliance obligations, risks, and controls throughout the enterprise. That's what Risk Intelligent compliance can offer.

A terminological note

"Inherent risk" refers to the risk posed by a risk event before a company addresses it — that is, the risk to the company in the absence of any internal controls, business processes, or other actions it might take to either reduce the likelihood of the event or mitigate the severity of its impact on enterprise value.

"Residual risk," sometimes termed "exposure," is the risk that remains after the company has installed internal controls, business processes, and/or other efforts to monitor, manage, and mitigate the inherent risk. These efforts may aim to decrease the likelihood of a risk event, lessen its potential impact on enterprise value, or both.

Risk "tolerances," sometimes called risk "limits" or "targets," are formally defined boundaries to the extent of residual risk that a company's leaders are willing to accept. The goal of a company's ERM program is to keep residual risk in each class of enterprise risk "within tolerance" or "within limits."

Inherent risk, residual risk, and risk tolerances may be expressed either quantitatively or qualitatively, depending on the nature of the risk. For instance, financial risks and risk tolerances are often stated in terms of their monetary value, while risks that are less readily quantified, such as risks to reputation, may be assigned ratings such as "high," "medium," and "low." (However, see the discussion of analytics on page 15 for approaches to quantifying reputational and other nonfinancial risks.)

The building blocks of Risk Intelligent compliance

Risk Intelligent compliance has three core attributes. It aligns compliance investments with compliance risk ratings and business priorities. It recognizes the scope and magnitude of compliance's potential impact on value. And it takes advantage of a company's compliance strengths to pursue "upside" value. To accomplish these things, the Risk Intelligent CCO works with ERM leadership to embed an enterprise perspective into compliance risk management; helps the company's leaders understand compliance's potential impacts on multiple value drivers; and actively looks for ways to leverage the company's compliance capabilities to grow enterprise value.

Stripped to its essentials, Risk Intelligent compliance is distinguished by three core attributes:

- It aligns compliance investments with compliance risk ratings and business priorities
- It recognizes the scope and magnitude of compliance's potential impact on value
- It takes advantage of a company's compliance strengths to pursue "upside" value

Absent any one of these attributes, a company might still be able to manage compliance risks to within acceptable tolerances, but it may miss out on the extent of the benefits that adopting all three can deliver.

Aligning compliance investments with compliance risk ratings and business priorities

An important part of any CCO's job is to help the business understand where and how it should allocate its compliance investments (including money, people, and effort). This can be a Herculean task, especially at companies with less-than-progressive attitudes toward compliance. It's the rare CCO who hasn't experienced at least some pushback from people demanding to know why the business should invest people, time, and money in what is often perceived as a non-revenue-generating staff function.

Fortunately, the Risk Intelligent CCO has an asset that can help him or her meet such challenges with confidence: a risk intelligent approach to the compliance risk assessment process.

The compliance risk assessment process is a company's core methodology for identifying its compliance risks and determining their relative importance to enterprise value. It's typically owned and executed by the compliance function, whose responsibilities may include developing and maintaining the company's compliance risk management framework, working with business-unit and functional stakeholders to identify and assess compliance risks, compiling a compliance risk register that itemizes the company's key compliance risks and requirements, and prioritizing the company's internal control, oversight, and mitigation efforts as well as overseeing their deployment and maintenance.

Although it's theoretically possible to fold compliance into a company's broader ERM program, most companies wisely choose instead to manage compliance risk with a separate compliance risk management program that runs in parallel with ERM. The reasons for this revolve around the specialized nature of compliance and the size of the impacts with which it typically deals. Many compliance requirements are so complex, and require such detailed contextual knowledge to understand and interpret, that companies usually find that they need a distinct compliance risk management framework to accommodate the subject matter's many nuances. In addition, because many ERM programs are designed around risks whose materiality impacts typically far exceed the direct cost of most compliance incidents (e.g., fines, penalties, and/or remediation costs), the wholesale application of high-level ERM processes to a direct-cost view of compliance risk impacts could push most compliance risks below ERM materiality thresholds entirely. A financial services company, for example, may deal largely in credit, market, liquidity, and other risks whose impacts can run into the hundreds of millions of U.S. dollars, while most of its compliance risks' potential direct costs may be much smaller.

But even though operationally separating the two programs makes sense, the frequent problem is that the compliance program may operate, not in parallel with the ERM program, but in virtual isolation from it. When this happens, the company's compliance risk management framework and process may be developed and executed with little regard for its overarching risk management and strategic priorities. And this means that the compliance program's outputs and recommendations may diverge, sometimes substantially, from the company's business priorities.

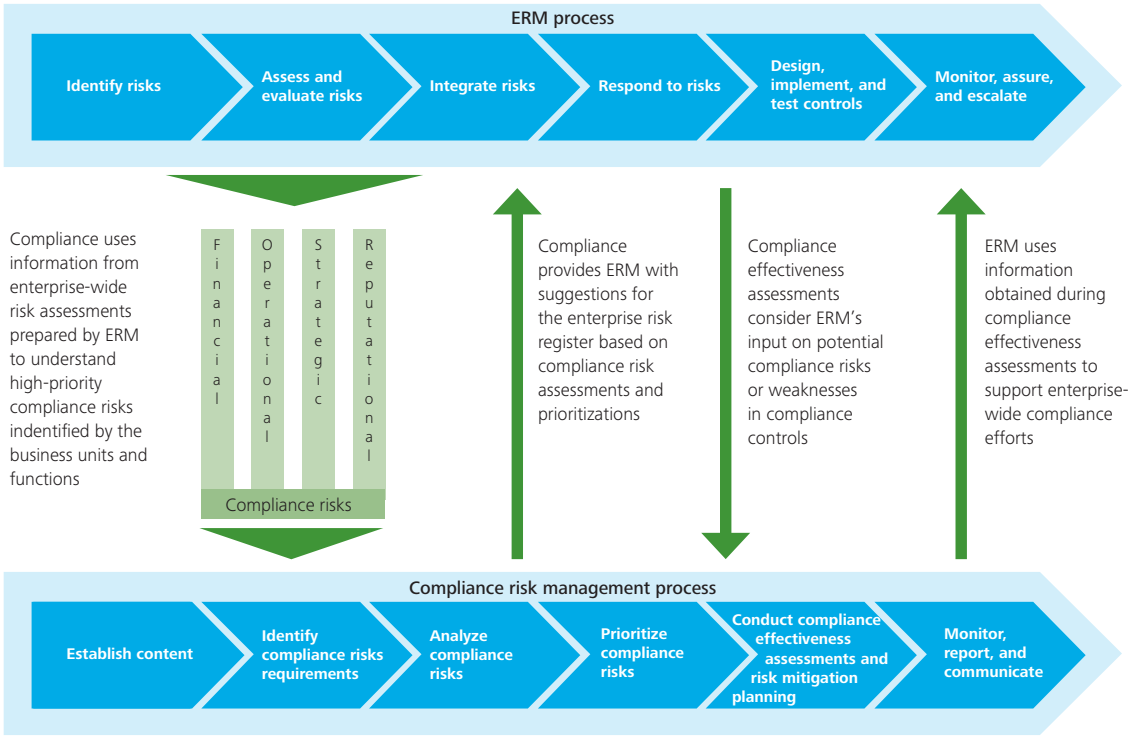
Needless to say, divergence between compliance risk management priorities and business priorities undermines Risk Intelligent compliance at its source. To guard against it, the Risk Intelligent CCO, in concert with ERM leadership, should develop processes and procedures that embed an enterprise perspective into the compliance risk management program. Operationally, this entails establishing information-sharing touchpoints between the compliance risk management process and the ERM process at specific stages in each process (see Figure 1). Important outcomes to aim for are:

- **Consistency between the compliance risk management framework and the ERM framework.** The compliance risk management framework should adhere to the ERM framework's enterprise-wide standards for defining, assessing, managing, and reporting risk. Elements that should be consistent across both include the risk taxonomy (i.e., the company's categorization of risks into discrete classes); risk definitions and terminologies (e.g., guidance on what constitutes "high," "medium," and "low" residual risk); methodologies and templates for risk assessment, testing, monitoring, and remediation (which should be similar in structure, if not in their subject-matter-specific content); and risk reporting conventions (e.g., a standardized reporting template and a reporting schedule that coordinates with ERM's).
- **Materiality thresholds for compliance risks that consider how the company's ERM and business priorities might affect the treatment of specific compliance risks.** Viewing compliance risks through an ERM lens can help compliance professionals set compliance risk materiality thresholds that reflect overarching business priorities. For instance, the ERM program might identify "being late to market" as a key enterprise risk. The compliance function would consider this as a factor when it develops materiality thresholds and oversight priorities for compliance obligations that could affect speed to market, such as product development regulations that are provisional or unclear.
- **A list of the company's key compliance risks along with an inherent risk rating and a residual risk rating for each.** This list is the Risk Intelligent CCO's touchstone for prioritizing compliance risks, efforts, and investments. Inherent risk ratings indicate the importance of each risk to the enterprise, while residual risk ratings should drive the prioritization of the company's testing and remediation efforts. If appropriately informed by ERM, each compliance risk's inherent risk and residual risk ratings will reflect overall enterprise priorities rather than local ones. This gives the CCO a strongly defensible basis for allocating the compliance function's time and resources and for recommending compliance investments to the rest of the business.

As its reciprocal contribution, the compliance function should bring a compliance perspective to ERM's treatment of enterprise risks. For example, compliance should keep ERM informed about compliance-related matters that could affect leadership's view of specific enterprise risks. Compliance should also identify high-priority compliance risks for ERM to include in the enterprise risk register, as well as share relevant information from compliance risk assessments to support any ERM-driven compliance efforts.

Aligning a company's compliance risk management program with its ERM program is a critical first step toward Risk Intelligent compliance. It's nothing less than the mechanism that allows the Risk Intelligent CCO to establish, strengthen, and validate the link between compliance and enterprise value.

Figure 1. Aligning compliance risk management with ERM



Both the ERM process and the compliance risk management process are iterative, with the end of the process in one period feeding into the beginning of the process during the next period.

Recognizing the scope and magnitude of compliance's impact on value

As mentioned above, one reason many companies separate compliance risk management from ERM is that the immediate direct cost of most compliance failures would put many compliance risks below ERM materiality thresholds. However, the flaw in this viewpoint is that direct cost may represent only a small fraction of compliance's total impact on enterprise value. The collateral damage a compliance failure can deal to a company's reputation, operations, and strategy can far exceed its direct financial cost. What's more, a company need not have an actual compliance failure to suffer compliance-related value loss. If a company has poor relationships with regulators, for instance, it may experience negative impacts ranging from more frequent audits to a higher cost of capital due to marketplace concerns about possible regulatory action.

Most boards and executives do recognize that compliance incidents can have reputational, operational, and strategic impacts as well as direct financial ones (see sidebar, "Compliance risk by any other name," for some examples). Most also acknowledge that the consequences, at worst, can be devastating. Regulators, governments, and other interested parties can impose crippling fines, file multbillion-dollar lawsuits, require independent monitors and overseers, revoke a company's license to operate, restrict strategic activities such as overseas expansion or merger and acquisition (M&A) deals, debar a company from doing business with government, bring felony charges against executives and board members, and so on.

So why do many CCOs still have trouble garnering funds for badly needed compliance investments until and unless something big breaks? One reason, frankly, may be that truly "devastating" potential impacts hardly ever materialize in real life. Fines can be negotiated down, lawsuits may be settled or won, licenses can be regained, and, while some business leaders have indeed been charged, convicted, and imprisoned for regulatory violations, they represent only a tiny fraction of the total. Given that the big blows are rare and that the smaller blows may not add up to material significance, leaders at many companies may view the foregoing simply as a cost of doing business, and be reluctant to invest more in compliance risk management than the bare minimum needed to keep that cost to a supportable amount.

The Risk Intelligent CCO can make at least two replies to this. The first is that "bad" things can and do happen to "good" companies. Even though "devastating" compliance incidents may be rare, their consequences, when they do occur, can be so severe that the risks should be examined and addressed no matter how improbable they are. Many extremely-high-impact compliance incidents may be the kind of "once in a lifetime" event that everyone knows could happen, but few believe will happen to them. The Risk Intelligent Enterprise should be one of those few.

The other possibility the CCO should raise is that the company's compliance risk exposures are actually greater than its historical risk assessments may indicate. In other words, what may currently look like an acceptable level of residual compliance risk could actually, if appropriately evaluated, exceed tolerance by a considerable margin. This can occur if, for instance, a company's compliance risk assessments fail to consider compliance's potential impacts on seemingly unrelated value drivers. It can also happen if compliance risk assessments are influenced by factors that encourage a rosier-than-warranted view, such as the misleading sense of security that can arise at companies that have had only a few compliance incidents over a sustained period of time.

The possibility of biased assessments brings up the larger issue of how CCOs can be confident that compliance risk ratings, especially ratings that use qualitative metrics, accurately reflect the "real" extent of each risk. In fact, the same issue may exist across all risk classes: In most risk management methodologies, the assessment of impacts on "intangible" value, such as reputational value, essentially comes down to someone's opinion. Fortunately for the Risk Intelligent CCO, the historic problem of quantifying impacts on "intangible" value can now be addressed through business analytics — a potentially invaluable capability that many companies are already exploring for use in other parts of the business.

The modern discipline of analytics, fueled by advances in computing speed and capacity, makes it possible to develop quantitative metrics for a host of factors that have long been viewed as unquantifiable. In a risk management context, this means that CCOs can use analytics to (among other things) help explode the myth that impacts on "intangible" value cannot be rigorously measured or managed. For example, analytics can help define and track a composite metric, based on observable indicators such as media mentions and customer feedback, that reflects the state of a company's reputation in quantitative terms. Using techniques such as historical analysis and predictive modeling, analytics can also forecast the potential reputational impacts associated with a given compliance incident, as well as the likely financial consequences of the reputational impacts.

Compliance risk by any other name

Areas in which compliance incidents can compromise value include:

- **Reputation.** Damage to reputation can have a variety of detrimental impacts, including revenue loss from customer flight, opportunity costs associated with difficulties in new customer acquisition, a higher cost of capital due to lender and investor nervousness, and so on.
- **Operations.** Regulatory sanctions can affect operations in ways ranging from requiring minor process adjustments, to naming a government-appointed monitor to oversee critical aspects of the business, to shutting down operations entirely. Less often mentioned, but potentially just as troublesome, are the operational demands of addressing compliance incidents when they arise. Responding to and managing investigations and subpoena demands, negotiating with authorities, tracking down information for audits, organizing public relations campaigns, and similar activities take time, resources, and money — not to mention valuable management and employee focus and attention — that could otherwise have been spent on growing the business.
- **Strategy.** Regulatory sanctions can strike at the heart of a company's ability to plan and execute an effective strategy. For instance, regulators and governments have been known to restrict corporate M&A or sales activities, or debar or suspend government contract opportunities, until outstanding compliance issues are resolved. Adverse regulatory rulings may also dissuade institutional investors from lending a company capital to expand its operations.
- **Finance.** A compliance incident may result in explicit financial costs due to fines, penalties, and remediation efforts. The indirect impacts, mediated through effects on areas such as reputation, operations, and strategy, can include additional financial losses in both the short and long term.

The good news is that the same paths that link compliance failures with potential value loss can also lead from effective compliance to value preservation and creation. In a global economy where compliance truly matters, a strong compliance record can become a marketplace differentiator and a competitive advantage. The possible benefits don't stop there, either. As the following section describes, strong compliance capabilities can allow a company to seize "upside" business opportunities that may be off-limits to less capable peers.

That said, it takes more than just analytics to help stakeholders appreciate compliance's far-reaching effects on enterprise value. The Risk Intelligent CCO is responsible for driving the point home. Through influence and advocacy — backed up by an ERM-aligned compliance risk management program — the CCO can play a critical role in helping the business recognize the potential impacts of compliance incidents across all dimensions of value and understand the implications at an enterprise level.

Taking advantage of compliance strengths to pursue "upside" value

Compliance risk management is often seen entirely in terms of "keeping the business out of trouble." But although keeping the business out of trouble is important, it's only half the story. The other half is the potential for a company's strengths in compliance risk management to help create new value. How? By opening the door to opportunities that companies with weaker compliance capabilities might consider too risky to pursue.

For example, let's say that a company is contemplating a business opportunity in a country where bribery is a common and expected business practice. The revenue potential could be huge — but so is the inherent risk of violating anti-corruption regulations such as the U.S. Foreign Corrupt Practices Act (FCPA), the U.K. Bribery Act, and similar regulations in other countries. If leaders lack confidence in the company's anti-corruption controls, processes, and oversight procedures, they might forego the opportunity, reasoning that the increase in residual compliance risk would outweigh the potential revenue gains. At a company with strong anti-corruption programs and controls, however, leaders might well embrace the opportunity, judging the company's corruption-related risk management practices up to the job of keeping the related residual risk within tolerance.

Most CCOs will probably know of several strategic initiatives at their own companies that are grounded in the presumption of effective compliance risk management. Besides operations in countries known to be high-risk for FCPA violations, pursuits that rely heavily on a company's compliance capabilities can include new product development, M&A transactions, facilities construction and expansion, business partnerships and joint ventures, contracting with government entities, and more. And of course, the need for effective compliance remains even after strategic initiatives mature into "business as usual."

Naturally, to seek new value through effective compliance risk management, leaders must be reasonably certain that compliance risk management is effective. Risk Intelligent compliance can support effectiveness by guiding an appropriate amount of effort to each compliance risk, neither too much (which wastes resources) nor too little (which may result in unacceptable control weaknesses). In addition, because Risk Intelligent compliance views compliance risks from an ERM and business perspective, leaders can be confident that the company's compliance risk management efforts are aligned with its overall business priorities.

The Risk Intelligent CCO will counter any tendency to take compliance for granted by promoting a healthy regard for compliance's essential contribution to enabling strategic execution. In conversations with fellow leaders, the CCO may highlight instances where the company's compliance capabilities have already helped advance strategic goals. The CCO should also help the company prepare for the future by planning for anticipated as well as current compliance needs.

The more effective a company's compliance risk management program, the greater the inherent compliance risk it can assume without exceeding leaders' tolerance for residual compliance risk. This is why effective compliance risk management is central to profitability and growth.

Toward Risk Intelligent compliance

Achieving Risk Intelligent compliance often entails a fundamental cultural transformation. The Risk Intelligent CCO can support this transformation by:

- Getting the top brass on board, especially the CRO, CEO, and the board of directors
- Taking the company's bearings to understand the current state of compliance
- Developing an ERM-aligned compliance risk management program as a critical first step
- Aligning the compliance function's activities with compliance risk management priorities
- Lobbying for technology to improve compliance efficiency and effectiveness
- Piggybacking on the work of other groups, particularly internal audit, but also the business units and functions, to reduce duplication of effort
- Fostering a culture of compliance in which employees and management in the business units and functions accept their responsibility for maintaining compliance
- Participating in strategic planning to help leaders take compliance into appropriate account

More than just a set of policies and procedures, Risk Intelligent compliance is a cultural ethic that recognizes and practices effective compliance risk management as a business asset. This attitude can be a radical shift from the way most companies see compliance today. To move a company toward Risk Intelligent compliance, the CCO will need to rally stakeholders across the organization, including executive peers, business-unit and functional leaders, and the board of directors. Here are some steps that can help CCOs get started.

Get the top brass on board

The road to Risk Intelligent compliance can be much less rocky if the CEO, CRO (or equivalent ERM leader), and the board of directors understand what the CCO is trying to do and why they should want to help. Because Risk Intelligent compliance requires communication between the compliance risk management program and the ERM program, the CRO's engagement is a prerequisite to the effort. Luckily, the CRO's shared interest in improving risk management effectiveness can make Risk Intelligent compliance a relatively easy sell. Any sticking points are more likely to arise in the details of how and when compliance and ERM will communicate than in the question of whether or not they should. It's wise, therefore, for the CCO to be prepared to discuss at least some of the operational implications in initial conversations with the CRO.

The CEO's role in supporting Risk Intelligent compliance is to empower the CCO with the authority needed to drive meaningful change, as well as to provide the necessary investment, political support, and, if needed, enforcement. First, however, the CEO will need to be convinced that the benefits of Risk Intelligent compliance are likely to outweigh the costs. The CCO can address this with a business case describing the risk management benefits of robust compliance processes, as well as the (potentially substantial) collateral benefits of cost reduction and revenue enhancement. With respect to cost reduction, the CCO should commit to pursuing continuous efficiency and effectiveness improvements as an ongoing part of the effort. (The CCO also should describe any up-front investments that may be needed, such as the purchase of more effective technology to replace spreadsheet-based tracking and reporting). With respect to revenue enhancement — a claim that may meet with more initial skepticism — the CCO can point to specific examples of revenue-generating initiatives where compliance has been a key enabler. The CCO may also give examples of additional strategic opportunities that Risk Intelligent compliance, by improving the organization's control over compliance risk exposures, can bring within reach.

Finally, the board of directors can help keep the company moving toward Risk Intelligent compliance by holding management accountable for results. Here, the CCO's task is to set expectations, develop metrics, and establish milestones that are both substantive and realistic, possibly in the form of a multiyear master plan. Given that more boards would rather spend more time on risk management than on compliance, CCOs may find it helpful to frame their discussions with the board in the context of the organization's broader ERM program.

Take the company's bearings

Like any transformation, the pursuit of Risk Intelligent compliance begins with understanding the current state. Important questions to ask include: What are the company's current compliance obligations and risks? Who owns each risk? What controls are in place against them? How does the organization respond to control failures? How are remediation priorities set? How is monitoring and auditing conducted? What supporting technologies are used? Depending on how effective compliance oversight has been in the past, the effort to uncover these and other basic facts may range from refreshing prior efforts to performing a full-blown compliance risk inventory and assessment.

Develop the ERM-aligned compliance risk management program

To reiterate an earlier point: Coordinating compliance risk management with ERM gives CCOs the operational basis for establishing, strengthening, and validating the link between compliance and enterprise value. How a CCO accomplishes this at any particular company will depend greatly on internal organizational dynamics. For insights on how to maintain effective cross-communication with ERM, the CCO may want to look at the way the finance function interacts with ERM to manage the company's financial reporting risks.

Align the compliance function

The process of aligning compliance activities and investments with business priorities starts with the compliance function itself. The CCO should allocate the compliance function's activities across the company's compliance risks according to the relative importance of each compliance risk to enterprise value. In some cases, this may mean deploying people and infrastructure to countries, programs, and/or activities where greater investment seems counterintuitive. In others, it may mean scaling back on one or more "sacred cows." In either case, the CCO should be able to back up his or her decisions with reasons that tie solidly back to ERM priorities.

The corollary is that CCOs themselves should prioritize requests for investments in the compliance function based on their expected risk management benefit. Barring obvious infrastructural or resource gaps, the choice of what to ask for first may sometimes come down to a frank judgment call. Our experience suggests, however, that many CCOs are likely to put a high priority on improving compliance's enabling technology.

Lobby hard for effective technology

The "right" technology, both within and outside the compliance function, can go a long way toward improving compliance efficiency and effectiveness. Automating controls, for instance, can help lower costs and increase reliability, especially if the controls are first rationalized to reduce duplication. Companies can also avail themselves of a growing array of tools to support the compliance risk management process, some stand-alone, some sold as part of larger "enterprise governance, risk, and compliance" (eGRC) solutions.

Over the past few years, many compliance tools have added new capabilities that can greatly aid in both execution and oversight. Among these newer features:

- Automated monitoring of regulatory releases, sometimes coupled with business process management tools to automatically alert responsible parties to relevant changes
- Workflow capabilities to facilitate compliance process execution and tracking and to promote individual accountability
- Integrated "front end" interfaces that allow users to execute, document, and track compliance activities in multiple areas from a single point of access
- Automated reporting and dashboarding tools that can consolidate compliance information from sources across the enterprise and display key compliance risk and performance indicators in a board-friendly format
- Analytics and visualization tools to help guide risk and business decision making

The usual caveats about technology apply. A technology solution is only as effective as the process it enables; much of the benefit depends on managing change among users; and setting realistic expectations is vital to the perception of value. However, if effectively implemented and used, today's compliance tools hold the potential to drive substantial improvements in both information quality and process efficiency.

Piggyback on each other's work

Looking for ways to reduce duplication of effort with other internal groups can help a CCO stretch the compliance function's limited budget and resources. In particular, the CCO should enlist internal audit in supporting compliance oversight by testing and auditing compliance-related internal controls and business processes. Compliance personnel can advise internal audit on what tests would be most useful to the compliance function, as well as on what tests might be better left to the compliance function's specialists to perform. Although the compliance function may still carry out its own tests and monitoring procedures in some domains, including tests to validate selected findings by internal audit, a thoughtful look at the current overlap with internal audit will likely identify at least some opportunities for alignment.

A CCO may also approach the functions and/or business units to discuss more efficient ways to share responsibility for compliance-related activities. For instance, the compliance function may be able to use some of a business unit's built-in quality programs, such as a robust pre-implementation testing program for new technology systems, as a factor in a compliance risk assessment. Another possible tactic may be for business-unit employees to document certain compliance information as a standard process step, or to configure the business' enabling software to record the information automatically.

Foster a culture of compliance

Changing corporate culture can take years — meaning that the sooner the CCO tackles the cultural aspect of Risk Intelligent compliance, the sooner the company may start to see results. CCOs should expect to work with the office of the CEO, as well as human resources (HR), legal, and communications, to supervise the change initiative and supply compliance-specific guidance as needed. Important areas to address include:

- **Performance management and compensation.** One way to encourage Risk Intelligent compliance is to tie appropriate individuals' rewards to important compliance objectives. The compliance function can help identify which roles represent the company's "hottest" compliance seats and aid the rewards group in developing compliance performance metrics for these roles.
- **Training.** People can only comply to the extent they know how. The compliance function can identify training needs and audiences, help tailor curricula to particular groups, and deliver centrally deployed training initiatives (which may be complemented by local training).
- **Leadership development.** Top leaders throughout the organization must not only comply with applicable rules themselves, but also be prepared to discuss compliance-related issues with subordinates, regulators, governments, and the media. The compliance function can help coach current and prospective leaders in skills such as interacting with regulators and talking to the press.
- **Communications.** The compliance function can help clarify which stakeholders should hear what kinds of messages about compliance. It should oversee a recurring enterprise communication plan and work to keep the messaging fresh and relevant.

One message that CCOs may want to emphasize throughout the change program is that the responsibility for executing and maintaining day-to-day compliance rests with business-unit and functional employees and management, not with the compliance function.[10] The reason is simple: The extent to which a company transacts business in a compliant manner depends largely on the extent to which employees "on the ground" follow the rules. This is why the business units and functions are often termed the "first line of defense" against compliance incidents, with the compliance function the second line of defense.

A business' failure to acknowledge ownership of its responsibility for executing and maintaining compliance can cause CCOs immense frustration and potentially leave them vulnerable to scapegoating for compliance incidents. The support of the CEO and board is often critical in setting expectations for a culture of compliance and helping CCOs enforce accountability among business-unit and functional stakeholders. Transparency into compliance controls and processes can also be a great help. As one CCO put it: "If something is not done, I am happy to report who didn't get it done. … Transparency makes a compliance officer's job 100 times easier."[11]

Participate in strategic planning

The Risk Intelligent CCO should help leaders set a strategy that takes compliance into appropriate account by bringing relevant compliance perspectives to the strategic planning process. For instance, the CCO should explain what compliance obligations are associated with each of the strategic options being considered, help evaluate the likely compliance risk associated with each option, and describe the nature and extent of the investments that may be needed to maintain compliance risk exposures within acceptable tolerances under a variety of conditions. Once the strategy is set, the CCO should help the company understand and prepare to address compliance obligations that are expected to arise in execution.

Epilogue: The value of insight and control

Risk Intelligent compliance offers leaders important assets in their efforts to address their company's compliance obligations. It can give them enough insight into the company's compliance vulnerabilities to make effective business decisions about how each should be managed. By doing so, it can also give them enough control over compliance vulnerabilities to be able to take just "enough" of the "right" compliance risks to further the company's objectives.

For the CCO, Risk Intelligent compliance represents an opportunity to put compliance on a value-driven footing that can help it earn recognition as a valued and valuable business asset. For executive management and the board, it can mean greater confidence in their ability to understand and manage compliance risks in a manner that aligns with strategic goals. And for investors and business owners, it can help protect and enhance enterprise value by supporting effective compliance and by increasing the scope of viable growth opportunities.

One could discuss ad *infinitum* the merits of any particular law, regulation, or rule, but few would deny the social and economic imperative to pursue compliance with those that apply. Focusing on that fundamental element, and determining how to turn it to an organization's business advantage, is the essential mandate of the Risk Intelligent CCO.

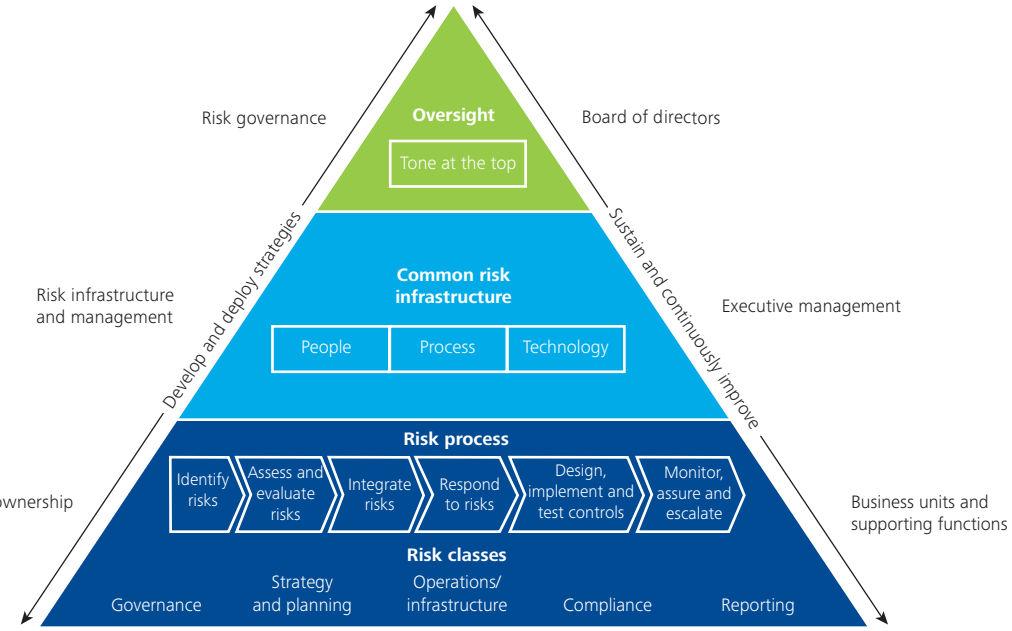
Appendix: A portrait of compliance in the Risk Intelligent Enterprise

How does Risk Intelligent compliance fit into the Risk Intelligent Enterprise as a whole? The short answer is that it's overseen by the board of directors as part of risk governance, enabled (mainly though not exclusively) by the CCO as part of risk infrastructure and management, and executed by the business units and supporting functions as part of risk ownership. However, the way regulators expect many companies to organize their compliance efforts introduces two wrinkles that set compliance apart from the other risk classes listed at the bottom of Figure 2.

The first distinction is that many companies are creating a centralized compliance function to consolidate oversight of the enterprise's compliance programs and execute the compliance risk management program. No equivalent function is likely to exist for the other risk classes. While the compliance function is a risk owner in its own right, it is also responsible for helping to maintain enterprise-wide consistency in how compliance risks are rated, controlled, documented, and reported. In effect, this makes it one of the CCO's main tools for establishing and maintaining a common risk management infrastructure for compliance.

The second distinction, which often applies even at companies without a centralized compliance function, is that the CCO or equivalent senior compliance executive may have greater access to the board of directors than executives associated with some of the other risk areas, such as the Chief Operating Officer. A CCO may find that board-level visibility can be an asset in matters such as advocating for compliance investments and strengthening relationships with executive peers.

Figure 2. Deloitte's Risk Intelligent Enterprise framework



Endnotes

[1] "The Economy, Compliance, and Ethics," Health Care Compliance Association and Society of Corporate Compliance and Ethics, February 2012. Available online at http://www.corporatecompliance.org/AM/Template.cfm?Section=Surveys&Template=/surveyform.cfm&survey=economy11.

[2] *Ibid*.

[3] "Stress, Compliance, and Ethics," Health Care Compliance Association and Society of Corporate Compliance and Ethics, January 2012. Available online at http://corporatecompliance.org/AM/Template.cfm?Section=Surveys&Template=/surveyform.cfm&survey=11Stress.

[4] U.S. Federal Sentencing Guidelines §8C2.5, "2011 Federal Sentencing Guidelines Manual," United States Sentencing Commission, November 1, 2011. Available online at http://www.ussc.gov/guidelines/2011_Guidelines/index.cfm.

[5] "2011 BDO Board Survey," BDO USA, LLP, 2011.

[6] Emmanuel Olaoye, "Evidence, access aid job security when compliance staff raise a red flag," Financial Regulatory Forum, Thomson Reuters Accelus, February 9, 2012. Available online at http://blogs.reuters.com/financial-regulatory-forum/2012/02/09/evidence-access-aid-job-security-when-compliance-staff-raise-a-red-flag/.

[7] Not all compliance incidents indicate an unacceptable weakness in the control environment. If a compliance incident's business consequences are not material, and if an appropriate assessment determines that the existing control environment is adequate to keep the risk of recurrence within tolerance, leaders may decide to leave the control environment as it is on the grounds that further reductions in the risk of recurrence would not be worth the additional investment.

[8] Based on the definition in "Compliance and the compliance function in banks," Basel Committee on Banking Supervision, April 2005. Available online at http://www.bis.org/publ/bcbs113.pdf.

[9] We use "compliance incident" to refer to the internal or external disclosure of compliance-related problems, including but not limited to compliance failures.

[10] Rarely, some companies may deploy compliance professionals to certain high-risk business processes. This, however, is exceptional.

[11] Nina Youngstrom, "Many Compliance Officers Face Growing Workload, Stress and Pushback From Execs," Health Business Daily, February 17, 2012. Available online at http://aishealth.com/archive/rmc020612-02.

Nine fundamental principles of a Risk Intelligence program

1. In a Risk Intelligent Enterprise, a common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organization.
2. In a Risk Intelligent Enterprise, a common risk framework supported by appropriate standards is used throughout the organization to manage risks.
3. In a Risk Intelligent Enterprise, key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the organization.
4. In a Risk Intelligent Enterprise, a common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities.
5. In a Risk Intelligent Enterprise, governing bodies (e.g., boards, Audit Committees, etc.) have appropriate transparency and visibility into the organization's risk management practices to discharge their responsibilities.
6. In a Risk Intelligent Enterprise, executive management is charged with primary responsibility for designing, implementing, and maintaining an effective risk program.
7. In a Risk Intelligent Enterprise, business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management.
8. In a Risk Intelligent Enterprise, certain functions (e.g., HR, finance, IT, tax, legal, etc.) have a pervasive impact on the business and provide support to the business units as it relates to the organization's risk program.
9. In a Risk Intelligent Enterprise, certain functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organization's risk program to governing bodies and executive management.

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.