ITCi Research Report

August 2007

The State of Accountability

Prepared by Jeff Grimshaw and Jan Lee

- Challenges
- Benchmarks
- Best Practices

Developed in conjunction with

CRA

ITCi
IT Compliance Institute™

ITCi Research Report

August 2007

Table of Contents

About the Report Authors

Jeff Grimshaw is a partner at CRA; where he's been for 14 years. He is an organizational effectiveness consultant working on IT and compliance-related issues in organizations such as Kaiser Permanente, KPMG, Goldman Sachs, and many others. He is co-author of the forthcoming book *Take Away Excuses! A Leader's Guide to Creating the Conditions of Accountability*, and co-founder of Paul's Kids (http://www.paulskids.org), a Vietnam children's charity.

Jan Lee has been with CRA for 12 years and leads CRA's research practice. She conducts research addressing diverse issues such as employee, internal client, and customer satisfaction; organizational effectiveness; and strategic alignment for a variety of organizations, including Merck, Con Edison, Cargill, Carlson Companies, and Kaiser Permanente. She is co-author of the *Customer Satisfaction Measurement Handbook* and has earned a Six Sigma Black Belt.

About the IT Compliance Institute (ITCi)

The IT Compliance Institute (ITCi) strives to be a global authority on the role of information management in corporate governance, risk management, and regulatory compliance. Through comprehensive research, analysis, and education, ITCi helps organizational leaders overcome the challenges of today's complex regulatory environment and turn compliance responsibilities into capital opportunities. For more information on the state of accountability and other governance topics, visit http://www.itcinstitute.com.

About CRA

For 20 years, CRA has helped leaders make smart communication choices in order to produce results. One area of focus is helping leaders assess and solve high-stakes accountability problems.

Acknowledgments

ITCi thanks the many members and readers who made this report possible with their survey responses, comments, and insight. We also wish to acknowledge the diligent efforts of ITCi's account management and production teams, including Deirdre Hoffman, Lesley Schwartz, and Huan Do, in bringing this report to light.

Research Methodology

Focus

This report addresses issues surrounding accountability for IT compliance. It is designed to benefit IT, business, and compliance managers who oversee corporate governance, reporting, compliance, and risk management by exploring best practices for creating conditions that support accountability and exposing the gaps between the current state of IT governance, compliance, and the desired state.

This research summary equips IT compliance leaders with: 1) ideas and practices from peers related to improving accountability, and 2) language and a framework for engaging senior business leaders in more productive conversations about compliance-related accountability gaps and resolution.

Methodology

In April 2007, ITCi and CRA invited thousands of IT, compliance, and business managers to submit information about the state of accountability in their organizations. A total of 218 individuals responded to the joint survey, which was based on an accountability model developed by CRA. CRA analyzed all 218 survey responses to produce the following report.

Respondent Profile

Respondents came from all over the globe; most work in North American organizations, but the group included respondents from Saudi Arabia, The Netherlands, and Romania. Both small and large organizations are represented, as well as commercial entities, government organizations, and universities.

What Is Accountability?

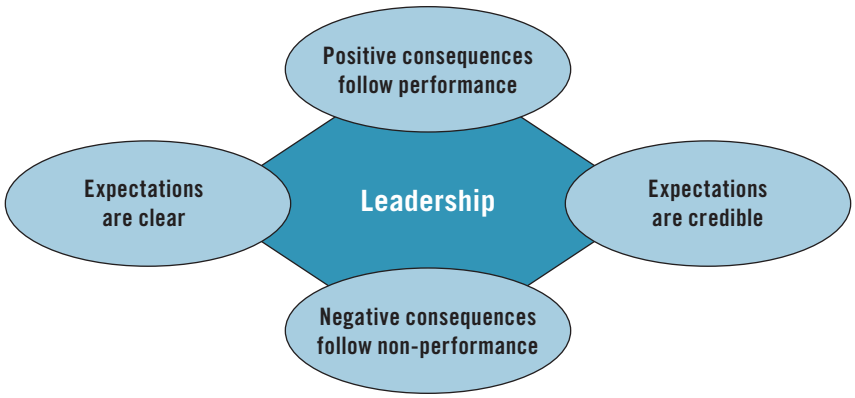
The business value of demonstrably, consistently compliant employee behavior is largely self-evident. While managerial strategy and goals might nominally support the business, it is employee adherence to the policies and procedures that enact those goals that is the ultimate test of managerial effectiveness.

All leaders and organizations struggle with accountability: particularly, situations in which employees fail to meet organizational needs and expectations. As legal and market forces have pressured companies to prove and improve specific governance, risk management, and compliance efforts, however, accountability has emerged as a linchpin for control enforcement and positive audits. Leaders have a responsibility to “take away excuses” and create conditions of accountability. Creating these conditions is, or should be, why managers are paid the big bucks.

What does it mean to create conditions of accountability? A predictive accountability model developed by CRA in partnership with a large North American insurance company and validated in dozens of organizations indicates that employees are accountable—that is, they do what's needed and expected—to the extent to which four factors are present:

- Expectations are clear to employees
- Expectations are perceived to be credible and reasonable
- Positive consequences are believed to follow compliant behavior
- Negative consequences are believed to follow noncompliant behavior

Accountability occurs when…



Conditions of Accountability Model © 2003 CRA, Inc.

CRA's research has shown that, when these four factors are in place, accountability failures are rare. If employees do not understand or support managerial expectations or they perceive that consequences are out of line with their behaviors, they frequently fail to do what is needed or expected.

Best Practices for Implementing Accountability

What can managers learn from organizations that have effectively created the conditions for IT compliance? Four factors emerge from this study as critical determinants of accountability:

1. Expectations are clear

When organizations create conditions of accountability for IT compliance, employees:

Are clear about specific behaviors they are expected to perform (and not perform). Employees have access to standards, policies, and procedures, written in plain language. There is a single, definitive, and up-to-date source of guidance, designed based on user input to ensure easy access. Additionally, employees have access to compliance information provided in a FAQ format that is responsive to questions that employees are actually asking about policies, procedures, and enforcement. Employees receive checklists and job aids—which provide significantly more practical value than posters, pens, and other trinkets that are staples of many compliance communication campaigns.

Understand how their compliance is evaluated. Employees recognize management priorities and what they need to do to get a positive evaluation. Additionally, they receive from their performance manager relevant, candid, and constructive compliance-related feedback on an ongoing basis—not just at formal review time.

Understand how compliance fits into the big picture and why it's mission critical. In many organizations, employees find it difficult to "connect the dots" between their day-to-day activities and the strategy or more esoteric mission and vision messages from senior leadership. Organizations that are successful in ensuring accountability make the "why" message explicit and repeat it frequently.

2. Expectations are perceived to be credible and reasonable.

In organizations where leaders have created conditions of accountability, employees:

Hear consistent compliance messages from senior leadership. As media oracle Marshall McLuhan famously stated, "the medium is the message." If employees don't hear senior leaders talking, and talking consistently, about compliance and explicitly linking it to business goals, the implicit message is that compliance isn't really important. Creating the conditions of accountability for IT compliance starts with tone at the top.

Participate in training that is leader-led (rather than led by compliance or HR or another support function). The source of information is a powerful message. Compliance messaging specific to job responsibilities and delivered by managers directly related to business functions is more effective than generic messaging delivered by central staff. To help leaders produce effective training, organizations must equip them to "look smart" in front of employees:

- Their information must be **privileged**. It's easier for managers and supervisors to look smart if they share information that has not previously been communicated to the masses. Since most employees in most organizations say their immediate leader is their preferred information source, give the preferred information source the ability to dispense the knowledge before directing employees to other channels.
- The information must be **simple and conversational**. If compliance messaging sounds like corporate-speak or otherwise like a compliance wonk or consultant wrote it, odds are, managers won't repeat it.
- The information must be **relevant**. It should squarely address the topics on which employees are seeking clarification, interpretation, and guidance.
- The information must be **consistent**. Inconsistent information unintentionally equips managers and supervisors with an excuse not to share.

Receive scenario-based training. Compliance training that delivers only general information about policies and practices has limited relevance to employees' day-to-day activities. Employees need ways to interpret policies requirements in terms of their actual work activities and settings, including "tricky" real-world situations in which answers aren't always black and white.

Know what to do when they don't know what to do. Organizations must equip employees with a "safe and efficient" means of asking questions and raising concerns when they're not sure what to do. In the absence of a credible, safe source of compliance help, employees will tend to make up answers as they go and hope for the best.

Receive credible guidance on balancing compliance against other business goals. Employees often perceive that acting in compliance contradicts corporate values, such as quality, speed, and cost management. They can perceive that this seeming contradiction places them in jeopardy. Organizational managers must create an atmosphere in which employees believe they can turn to leaders for guidance and that managers will provide trustworthy input.

Have frequent two-way dialogues with leaders about compliance issues. Consistent exchange of communication ensures that leaders know sooner, rather than later, when the organization is lacking conditions of accountability for compliance. Two-way communication allows management to move quickly to address accountability gaps. Managerial responsiveness to employee communications encourages employees to actively monitor and improve their own accountability environment.

3. Positive consequences follow compliance.

In organizations serious about compliance, leaders:

Reward and recognize compliance. Many organizations pursue negative consequences for employee noncompliance, but fail to provide positive consequences for compliance. However, the "carrot" can motivate behavior at least as powerfully as the "stick." Providing

consistent—and public—recognition for compliant performers can motivate stronger compliance across the organization. In the words of one survey respondent, one of the least effective ways of motivating compliance is, "Only implementing negative consequences and not allowing employees to earn or experience earned positive consequences."

Reward and recognize compliance based on how managers want the recipients to feel. Many business leaders are unaccustomed to talking about the taboo f-word—"feelings"—especially within the context of compliance. But employee "emotion" is an important and necessary criterion in accountability. Indeed, the power of any reward or recognition to motivate is only as strong as the emotions it elicits, and managers must consider factors such as employees' sense of status, inclusion, recognition, and other psychological drivers. For this reason, many organizations have found that increasing employee autonomy is the most powerful form of reward. For example, one survey respondent says: "Place no limits on access usage, as long as users refrain from bad behavior." A good "carrot" to motivate compliance, according to another respondent, is to, "display confidence in people when they meet your expectations."

Integrate compliance into performance goals and plans. If employees don't observe an explicit, measurable link between compliant behavior and performance evaluations (and accordingly, compensation and likelihood for promotion), managers cannot realistically expect employees to consistently focus on compliance—even if the employees are "good people."

Minimize or eliminate unintended negative consequences for top performers. In a majority of the organizations CRA has studied, employees report occasional negative consequences for compliance. This phenomenon frequently occurs in organizations in which performance management is poor. As a result, leaders "reward" the workers they trust to be compliant by giving them more work—to compensate for management's failure to motivate compliance from less productive performers.

4. Negative consequences follow non-compliance.

In organizations serious about accountability, leaders:

Withhold negative consequences until they have assessed the clarity and credibility of expectations. The capability to administer negative consequences must exist in any organization—and employees must be aware of it. In order to be effective, however, negative consequences should be administered to employees with clear expectations, who have the capacity and capability to deliver on those expectations, and who receive continuous and candid performance feedback.

Are consistent and predictable in administering negative consequences. As a rule, employees don't oppose negative consequences for non-compliant activities. But they do want consequences to be fair and consistent. As one survey respondent writes, "Be fair to the employee. All cases should be fairly investigated, and the outcome must be clear to the employee."

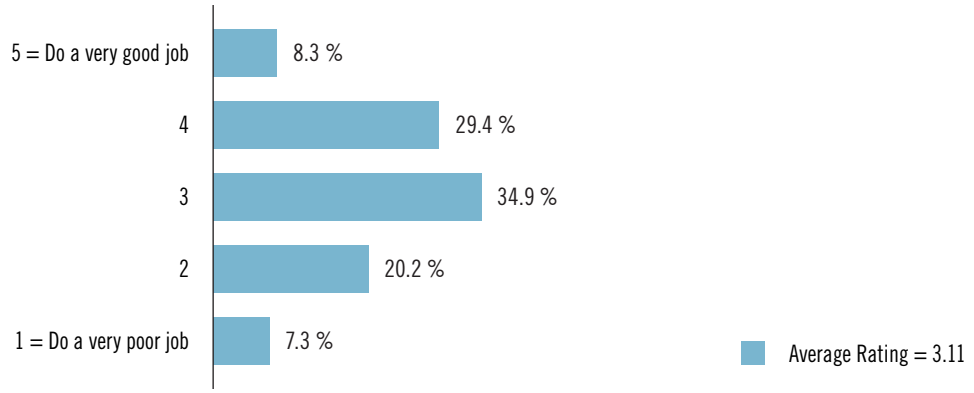
Carefully manage communication around "public hangings." Consequences send symbolic messages, intentionally or unintentionally. High-profile disciplinary actions are occasionally appropriate and necessary—for example, firing a worker for a significant and willful compliance breach. However, leaders must attempt to anticipate and account for the employee community's response to such "public hangings." For example, managers may need to develop and execute a communication strategy, ensuring the "buzz" created by a disciplinary action does not push underground employee discussions about their challenges associated with compliance.

Minimize or eliminate positive consequences for poor performers. In some organizations with accountability problems, noncompliant employees are unintentionally rewarded by managers who have been "trained" not to count on them and therefore give them less work. While avoiding confrontations with noncompliant workers might appear to be the path of least resistance for a particular manager, the unintended message this response sends to other organizational employees can absolutely undermine performance and contribute to a broadly noncompliant and nonproductive environment.

Follow through. Survey respondents stated that potential loss of job, loss of status, and loss of autonomy (for example, "loss of privileges, like home or internet access") are strong performance motivators and are therefore are useful negative consequences for noncompliance. In some organizations, however, leaders talk about "wringing necks," but don't act on their words. While a demonstration of managerial bravado may serve as a means of catharsis for frustrated executives, it is by no means an effective compliance solution. Survey respondents are clear that empty threats don't work. As one says, "You must be willing to make the difficult decisions. To date, there seems to be a reluctance to enforce compliance with negative consequences."

The State of Accountability

In general, how well does the organization hold employees accountability for complying with IT policies and procedures?



1. Companies struggle to hold employees accountable

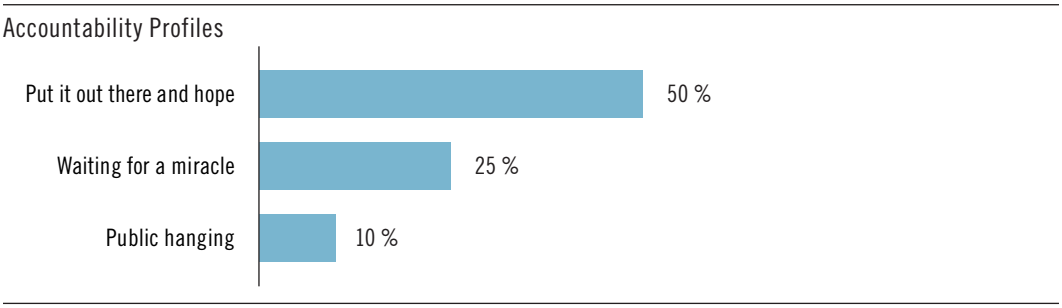
In survey responses, most managers report that their organizations do not have an effective approach for holding employees accountable for IT compliance. Only 8 percent of respondents report that their organization does a "very good" job of holding employees accountable for complying with IT policies and procedures. More than 60 percent say their organizations do a less-than-effective job.

What are some of the key issues organizations face?

- "It's hard to stop my people from installing their own versions of software, even when they, themselves, have a personal license, when our company drags its legs getting the licensed-to-us versions installed. Getting people to take the time out of their work day to carry out compliance-related activities (such as upgrading virus software, changing network configurations, migrating their laptops to new domains every time our firm acquires a new company, or is acquired, itself)."
- "Competing priorities and limited resources can be used as excuses. 'Compliance is a paper exercise' attitudes (includes lack of follow-up after setting up policies).
- "Getting employees to understand that compliance is an inherent part of their job, not an add on or afterthought."
- "Everyone claims to be too busy to do it right. It's just easier not to comply."
- "Diverse geographical locations and employee cultures are challenging."
- "Matrix reporting, reduced work force, and conflicting priorities limit accountability."

2. Organizations tend to fall into one of three primary accountability profiles

As demonstrated in this study, most organizations tend to approach accountability in ways that fit one of the following three profiles:



Put it out there and hope. Organizations in this profile typically do a passable job of creating awareness of IT compliance and governance requirements and provide the tools and resources employees need to comply. However, management has put in place few, if any, meaningful consequences around compliance. Based on survey responses, roughly half of organizations fall into this category.

What does this group tell us?

- "My life as a compliance/continuity/security/risk/kitchen sink manager is hell. Many different mediums and communication strategies have been deployed to educate employees about compliance requirements but too many of them are summary level PowerPoint pitches or flat narrative issued in bulletins. I'm crossing my fingers, holding my breath and praying to Allah, Buddha, Genesha, and Jesus that a new eLearning platform in the works will support more in-depth interactive and measurable coverage of the compliance material."
- "Incentive is largely avoidance of penalties or negative consequences."

Waiting for a miracle. Organizations in this profile haven't dedicated much effort or thought to holding employees accountable for IT compliance. One-quarter of survey respondents report that their organization does a generally poor job of implementing all four conditions of accountability.

What does this group tell us?

- "We create a heavy process in a vacuum and tell people they have to follow it but do not give them the guidance or resources they need to do so."
- "My IT staff has been rewarded in the past for lying their asses off on security questionnaires and hoodwinking the green auditors that cycle through the company. My IT staff needs serious negative consequences for non-compliance."

Relying on public hanging. This group encompasses organizations with a heavy-handed approach to consequences. The organizations don't set clear expectations; they don't explain the reasons behind compliance policies or provide the time, resources, or training needed to comply; and they don't reward those who abide by the rules. But they do an impressive job of making a public example out of those who—perhaps inadvertently—misstep. Ten percent of survey respondents fall into this group.

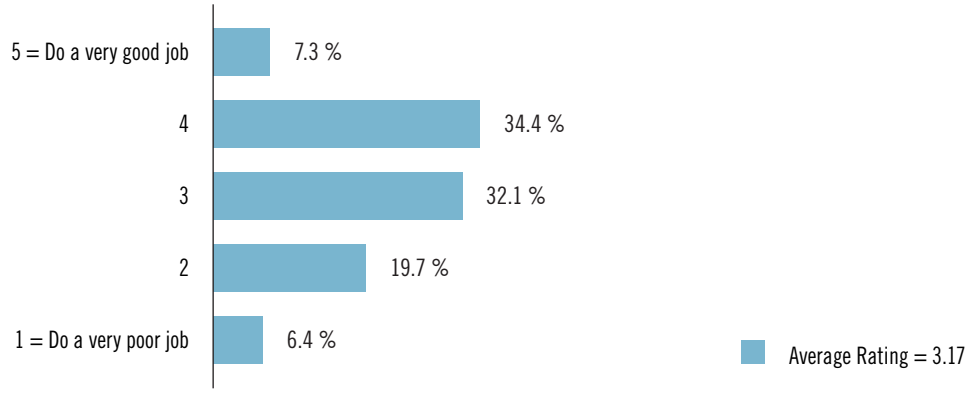
What does this group tell us?

- "Our organization has taken more of a stick than a carrot approach to compliance, partly because the compliance mandate comes from very senior management and may not be fully endorsed at the middle-management layer. Therefore, motivation for IT compliance has been negative, not positive."

3. Leadership fails to model accountability in their decisions or behavior

Nearly 3-in-5 respondents report a lack of leadership focus on accountability in their organizations, while only 7 percent note that leaders are doing a "very good job" of modeling accountability.

How well does organizational leadership model accountability in its decisions and behaviors?



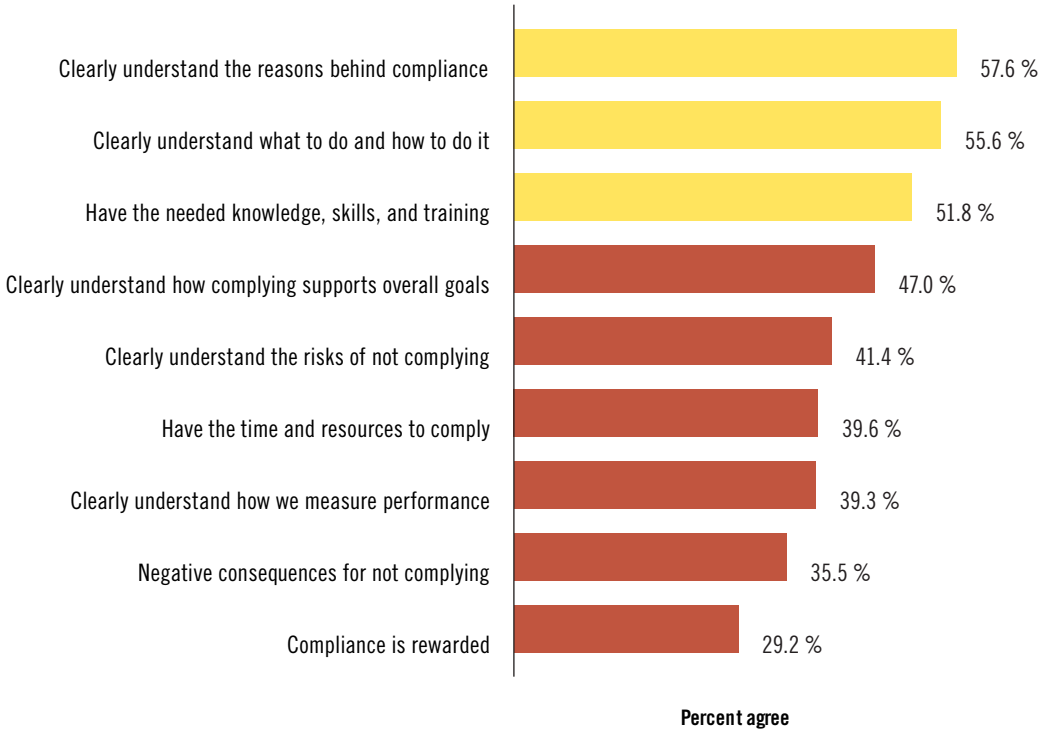
What do respondents say about leadership?

- "The message needs to come from the top down. Senior management has not weighed in on the issue yet, so efforts by IT to enforce compliance have been resisted."
- "Seniors leaders say they care but really don't; it's lip service. It's about the holy buck and forget about the risk."
- "My CIO sends out panicked emails or pulls together all-hands-on-deck meetings to deal with audits at the eleventh hour and pretends to not remember that everyone's been admonished all year long to implement or enhance compliance controls. He/she puts the technical staff on the spot for things that haven't been addressed when he/she knows good and well that security was relegated beneath a thousand other projects that were considered higher priority."

4. Responses across all survey items reveal gaps between the current state and best-practice findings

In organizations that are successfully holding employees accountable for IT compliance, levels of agreement to items that assess each of the four conditions of accountability typically approach 80 percent.

Summary of survey responses



In survey responses, levels of agreement are significantly below best-in-class targets. Respondents are most likely to note that their organizations do a fair job of making expectations clear and credible.

Responses for three items fall into a "yellow zone," reflecting moderate ratings:

- 58 percent of respondents report that employees in their organizations clearly understand the reasons behind compliance policies and procedures
- 56 percent report that employees in their organization clearly understand what to do and how to do it
- 52 percent of respondents report that employees in their organizations have the knowledge, skills, and training they need

However, responses to most items fall into the "red zone," reflecting large gaps between the current state and best-practice agreement levels. The lowest-rated items are related to consequences:

- Only 39 percent of respondents report that employees in their organization understand how their performance is measured
- Only 35 percent of respondents note that their organization effectively applies negative consequences to employees who don't comply with IT policies and procedures
- Less than 30 percent report that compliance is rewarded in their organizations

Recommendations

Driving compliance is a leadership imperative. But compliance leaders can't do it alone. As the findings make clear, leaders at all levels need to be able to engage and get support from senior leaders and other support functions (HR, training, etc.) with whom they are interdependent. Compliance leaders should use the "conditions of accountability" identified in this report as a framework for engaging senior leaders and other stakeholders in discussions about how to diagnose and address their accountability gaps.

Conclusion

The joint ITCi/CRA survey reveals that, of the more than 200 companies surveyed, 60 percent say that their organization does not have an effective approach for holding employees accountable and that leadership has not taken action to make accountability for IT compliance a priority. Half of respondents say their organization does a good job of communicating compliance-related expectations and making sure they're credible—but many of the same respondents say management hasn't yet done a good job of aligning consequences with behavior. Ten percent observe that management does well only on delivering negative consequences for noncompliant behavior, which is predictable behavior if the organizations haven't put in place the other three conditions related to expectations and positive consequences for compliance.

It's incumbent on leadership to change the compliance outlook. "Bad" employees are not the root cause of most compliance problems; most workers comply when the four factors of accountability identified in this report are in place. Making sure these four conditions exist is what leaders of best-practice organizations do.