KPMG FORENSIC[SM]

Integrity Survey 2013

kpmg.com

CONTENTS

Forensic Leadership Message

1

It is with great pleasure that we share with you the results of our Integrity Survey 2013, which provides an inside look into corporate fraud and misconduct as derived from the experiences and perceptions of more than 3,500 employees in the United States. Our survey is released at a time of great economic uncertainty and the importance of the data is compounded by the great need on the part of companies, regulators, and investors to understand better the risks of fraud and misconduct and work to ensure the effectiveness of ethics and compliance programs and related antifraud programs and controls.

Our 2013 survey builds upon insights gained from our previous Integrity Surveys conducted in 2009, 2005, and 2000. These surveys provide a unique perspective and help us gauge the progress organizations have made over the last thirteen years, as well as steps they still need to take to combat effectively fraud and misconduct. Some of our key findings in 2013 include:

- A majority of employees nationally – 73 percent – reported that they have observed misconduct in the prior 12-month period. More than half – 56 percent – reported that what they had observed could cause "a significant loss of public trust if discovered."
- The prevalence of misconduct that could cause a "significant loss of public trust if discovered" reported by employees in a number of industries saw a marked increase from the results of our survey in 2009 (e.g., Electronics, Software & Services, Chemicals & Diversified Industrials, Consumer Markets, Aerospace & Defense, and Real Estate & Construction).
- One of the most commonly-cited drivers of misconduct continues to be attributed to pressure to do "whatever it takes" to meet business goals. Other commonly-cited causes included not taking the organization's code of conduct seriously, having in place systems that rewarded results over means, and the fear of job loss if targets are not met.
- While the propensity to report misconduct to an ethics hotline has increased, employee willingness to look the other way and do nothing or to report misconduct outside the organization has also increased. Such results demonstrate a continuing need for organizations to enhance the effectiveness of their internal reporting mechanisms, especially in light of the provisions of various federal and state whistle blowing laws, including the recently enacted Dodd-Frank Act.
- Having in place formal ethics and compliance programs continues to make a positive difference. Employees who work in companies with programs generally reported more favorable results across the board than employees who work in companies without such programs.

We hope our survey provides you with a wide perspective as organizations consider their own exposure to fraud and misconduct risks and the effectiveness of the programs and controls they rely upon to mitigate such risks.

For more information about how KPMG's Forensic practice can help, please call us at 1-877-679-KPMG (5764) or visit us at www.kpmg.com.

Richard H. Girgenti

Richard H. Girgenti
Americas Practice Leader
KPMG Forensic

1.1 Executive Summary

The KPMG Integrity Survey 2013 results are based upon responses received from more than 3,500 U.S. employees spanning all levels of job responsibility, 16 job functions, 13 industry sectors and 5 thresholds of organizational size. **A majority of employees reported that they had observed misconduct in the prior 12-month period. More than half of employees reported that what they had observed was serious misconduct that could cause "a significant loss of public trust if discovered."** The survey found that:

- The levels of overall misconduct remained virtually unchanged, with a majority of employees nationally – 73 percent – reporting that they had observed misconduct in the prior 12-month period (74 percent in 2009, 74 percent in 2005).
- The prevalence of misconduct that could cause "a significant loss of public trust if discovered" increased. Of the employees surveyed in 2013, 56 percent characterized the misconduct they had observed as serious and possibly resulting in a significant loss of public trust, as compared to 46 percent in 2009 and 50 percent in 2005.
- The prevalence of misconduct that could cause "a significant loss of public trust if discovered" reported by employees in the Electronics, Software & Services industry represents a significant increase of 26 percentage points from the results of our survey in 2009, the highest increase of any industry measured. Other industries that experienced significant increases include Chemicals & Diversified Industrials (20 percentage point increase), Consumer Markets (20 percentage point increase), Aerospace & Defense (19 percentage point increase), and Real Estate & Construction (15 percentage point increase).
- The most commonly-cited driver of misconduct continued to be attributed to pressure to do "whatever it takes" to meet business goals (cited by 64 percent of respondents). However, we found thematic increases across the board in employee perceptions of the roots of misconduct, including a belief that the organization's code of conduct is not being taken seriously (60 percent), the fear of job loss over unmet goals (59 percent), and that employees would be rewarded for results and not the methods to achieve them (59 percent).
- The propensity to report misconduct to a supervisor remains high at 78 percent and has increased to 53 percent for reporting to an ethics hotline (up from 44 percent in 2009). However, employee willingness to look the other way or do nothing if they observed misconduct has increased (to 23 percent, up from only 6 percent in 2009). Similarly, employee willingness to report misconduct outside the organization has also increased to 26 percent (from 10 percent in 2009). Such results demonstrate a continuing need for organizations to enhance the effectiveness of their internal reporting mechanisms. This is especially important in light of the provisions of various federal and state whistle blowing laws, including the recently enacted Dodd-Frank Act, which established a "bounty program" for whistleblowers who raise concerns directly with the Securities & Exchange Commission.
- Having in place formal ethics and compliance programs continues to make a very positive difference as there is a strong correlation between ethics and compliance programs and positive perceptions of behavior. Employees who work in companies with programs reported fewer observations of misconduct, less toxic pressure to hit performance targets, and higher levels of confidence in management's commitment to integrity.


DATE
SALES
GROWTH
YTD

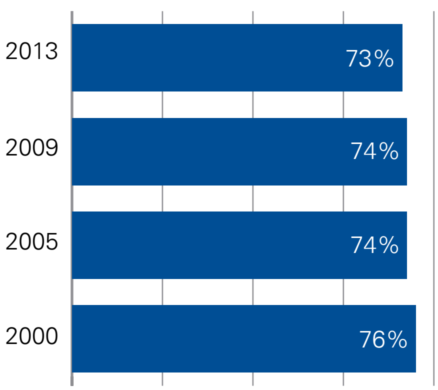
Overall Results

2

2.1 Prevalence and Nature of Misconduct

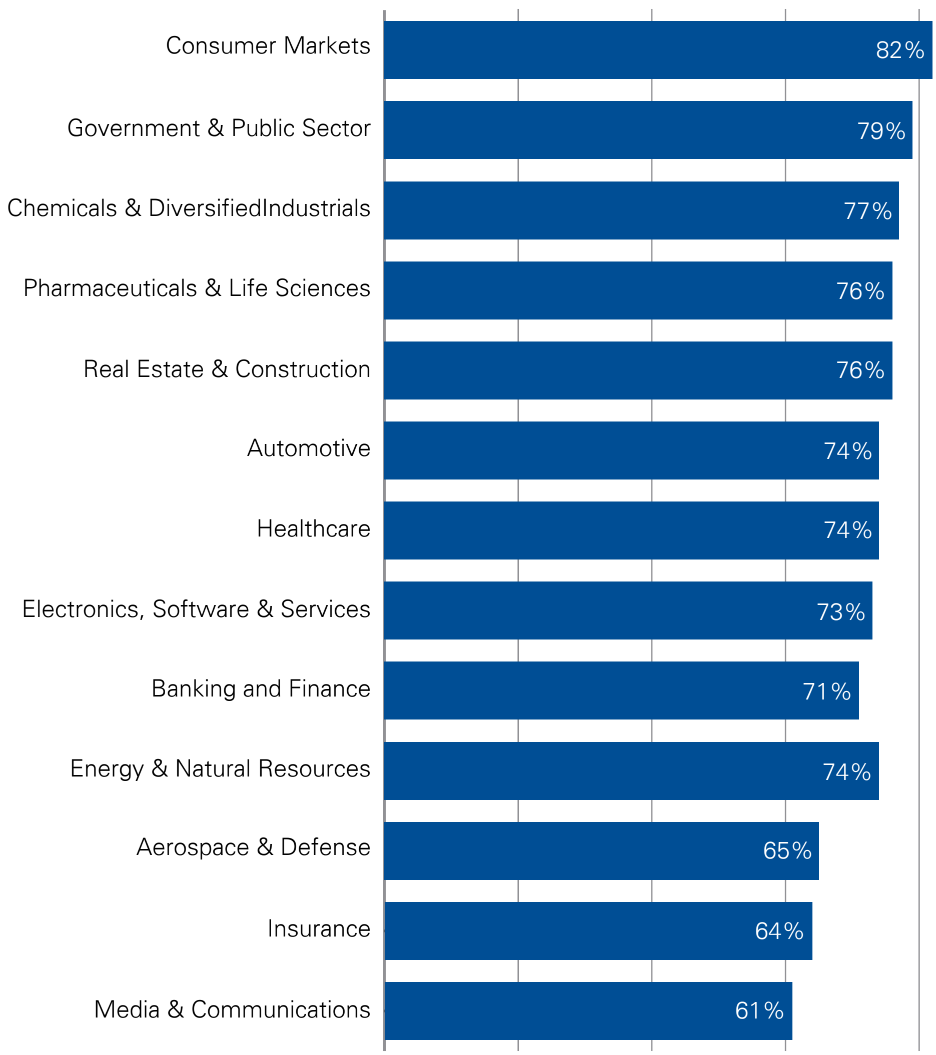
Prevalence of Misconduct
As our starting point, we wanted to gauge just how prevalent misconduct is in the workplace. We asked employees whether they had "personally seen" or had "first-hand knowledge" of categories of misconduct within their organizations over the prior 12-month period. A large majority –73 percent– reported that they had. As shown in the table below, this result falls directly in line with responses to the same survey question in previous years, marking no significant change in results.

Prevalence of Misconduct During the Prior 12 Months



Prevalence of Misconduct by Industry
When we examined the prevalence of misconduct across all industries, we generally found it to be high across all industries, fluctuating within a 20 percent range. Employees who worked in industries such as Consumer Markets, Forestry, Mining, & Natural Resources, and Government & Public Sector, reported the highest rates of misconduct overall. Employees in Media & Communications as well as the highly-regulated Insurance and Aerospace & Defense industries, reported comparatively lower rates of misconduct relative to other industries.

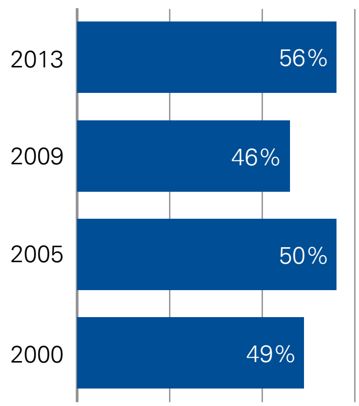
Prevalence of Misconduct by Industry during the Prior 12 Months



Seriousness of Misconduct

Next, to gauge the seriousness of observed misconduct we asked employees if they believed what they saw could cause a "significant loss of public trust" if discovered. More than half of employees—56 percent—answered affirmatively, representing a significant increase as compared with the 46 percent who answered affirmatively in 2009.

Prevalence of Misconduct that Could Cause a "Significant Loss of Public Trust if Discovered"



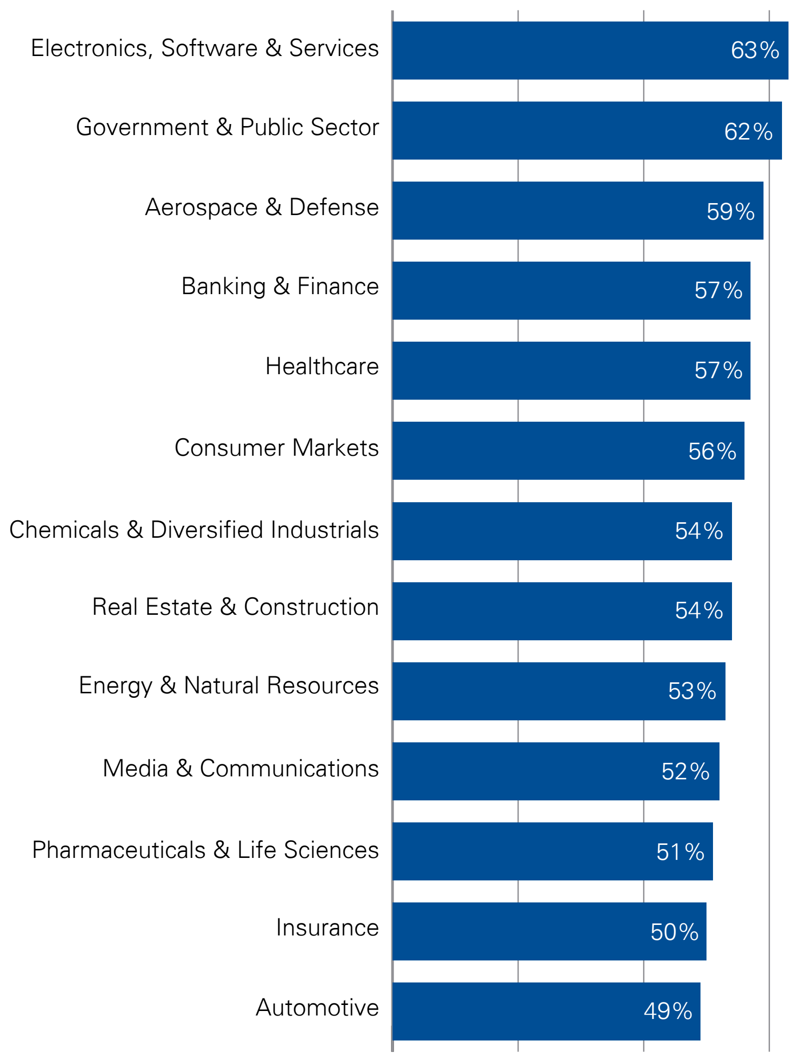
Seriousness of Conduct by Industry

When drilling down to an industry level, we found that the seriousness of misconduct varied across industries. For example, employees in the Electronics, Software & Services, Government & Public Sector, and Aerospace & Defense industries reported the highest instances of misconduct that could cause a significant loss of public trust. These results contrast with employees in the Pharmaceuticals & Life Sciences, Insurance, and Automotive industries, where the prevalence of serious misconduct was typically 10 percentage points lower.

Of particular note are results in various industries that represent a significant change from our 2009 survey results. In these industries, employees noted a higher occurrence of misconduct than was measured in 2009. For example, the prevalence of serious misconduct reported by employees in the Electronics, Software & Services industry represents a 26 percentage point increase from the results of our survey in 2009, the highest increase of any industry measured.

Similarly, the 2013 Consumer Markets industry data represent a 20 percentage point increase; the Chemicals & Diversified Industrials data represent a 20 percentage point increase; the Aerospace & Defense industry data represent a 19 percentage point increase; and the present result of the Real Estate & Construction industry data represent a 15 percentage point increase from our survey results in 2009.

Prevalence of Misconduct that Could Cause a "Significant Loss of Public Trust if Discovered," by Industry



Nature of Misconduct

While it is important to understand what type of misconduct is being observed, we asked employees to identify specific types of misconduct of which they had "first-hand knowledge" or had "personally seen." In doing so, we note that when allegations of organizational misconduct garner attention, the focus often tends to zoom in on one specific problem; however, experience tells us that integrity risks are not neatly segmented, and in fact, at any given time the nature of misconduct risk can be as diverse and fluid as the business itself. As such, we took a broader view by allowing survey respondents to select from among 42 relevant categories of misconduct that can undermine an organization's reputation for integrity.

As shown in the table below, these categories ranged from issues of financial reporting fraud, to a broader set of potential misconduct, all of which can undermine an organization's reputation for integrity.

Categories of Fraud and Misconduct Assessed in The Survey	
Compromising customer or marketplace trust by: • Engaging in false or deceptive sales practices • Submitting false or misleading invoices to customers • Engaging in anti-competitive practices (e.g., market rigging or "quid pro quo" deals) • Improperly gathering competitors' confidential information • Fabricating product quality or safety test results • Breaching customer or consumer privacy • Entering into customer contract relationships without proper terms, contracts, or approvals • Violating contract terms with customers	**Compromising supplier trust by:** • Violating or circumventing supplier selection rules • Accepting inappropriate gifts or kickbacks from suppliers • Paying suppliers without accurate invoices or records • Entering into supplier contracts that lack proper terms, conditions, or approvals • Violating the intellectual property rights or confidential information of suppliers • Violating contract or payment terms with suppliers • Doing business with disreputable suppliers
Compromising shareholder/organizational trust by: • Falsifying/manipulating financial reporting information • Stealing or misappropriating assets • Falsifying time and expense reports • Breaching computer, network, or database controls • Mishandling confidential or proprietary information • Violating document retention rules • Providing inappropriate information to analysts or investors • Trading securities based on "inside" information • Engaging in activities that pose a conflict of interest • Wasting, mismanaging, or abusing the organization's resources	**Compromising public or community trust by:** • Violating environmental standards • Exposing the public to safety risk • Making false or misleading claims to the media • Providing regulators with false or misleading information • Making improper political contributions to domestic officials • Making improper payments or bribes to foreign officials • Doing business with third-parties that may be involved in money laundering • Doing business with third-parties prohibited under international trade restrictions and embargos • Violating international labor or human rights
Compromising employee trust by: • Discriminating against employees • Engaging in sexual harassment or creating a hostile work environment • Violating workplace health and safety rules • Violating employee wage, overtime, or benefit rules • Breaching employee privacy • Abusing substances (drugs, alcohol) at work	**General:** • Violating company values and principles • Engaging in fraudulent or illegal acts

Because different job functions are more likely to be in a position to observe different types of misconduct, in the tables that follow we cross-tabulated the percentage of employees in specific job functions who reported observing specific types of misconduct. For each job category, several common types of misconduct were identified based upon the percentage of employees within a specific job functions that reported observing a category of misconduct.

Select Observations by Employees in Sales and Marketing Functions

	2013	2009
Engaging in false or deceptive sales practices	47%	27%
Improperly gathering competitors' confidential information	34%	20%
Violating contract terms with customers	29%	14%
Engaging in anti-competitive practices	32%	12%
Submitting false or misleading invoices to customers	30%	9%

Select Observations by Employees in Accounting and Finance Functions

	2013	2009
Breaching computer, network, or database controls	34%	22%
Entering into customer contract relationships without proper terms, contracts, or approvals	35%	18%
Stealing or misappropriating assets	30%	17%
Falsifying or manipulating financial reporting information	29%	13%

Select Observations by Employees in Purchasing and Procurement Functions

	2013	2009
Entering into supplier contracts that lack proper terms, conditions, or approvals	29%	26%
Violating or circumventing supplier selection rules	31%	24%
Accepting inappropriate gifts or kickbacks from suppliers	35%	23%
Violating contract or payment terms with suppliers	35%	20%
Engaging in anti-competitive practices (e.g., market rigging)	35%	12%

Select Observations by Employees in Research, Development and Engineering Functions

	2013	2009
Mishandling confidential or proprietary information	34%	24%
Engaging in activities that pose a conflict of interest	36%	22%
Accepting inappropriate gifts or kickbacks from suppliers	32%	13%
Improperly gathering competitors' confidential information	36%	11%

Select Observations by Employees in Operations and Service Functions		
	2013	**2009**
Wasting, mismanaging, or abusing the organization's resources	43%	44%
Violating employee wage, overtime, or benefit rules	42%	28%
Breaching employee privacy	39%	28%
Mishandling confidential or proprietary information	29%	22%
Falsifying time and expense reports	33%	21%

Select Observations by Employees in Manufacturing and Production Functions		
	2013	**2009**
Violating workplace health and safety rules	54%	47%
Discriminating against employees	54%	47%
Engaging in sexual harassment or creating a hostile work environment	50%	38%
Abusing substances (drugs, alcohol) at work	42%	26%
Fabricating product quality or safety test results	42%	23%

Select Observations by Employees in Quality, Safety and Environmental Functions		
	2013	**2009**
Violating environmental standards	48%	27%
Exposing the public to safety risk	46%	17%
Fabricating product quality or safety test results	55%	25%
Violating international labor or human rights	46%	7%
Doing business with third parties prohibited under international trade restrictions/embargoes	21%	3%

Select Observations by Employees in Technology Functions		
	2013	**2009**
Breaching employee privacy	39%	25%
Breaching computer, network, or database controls	38%	23%
Mishandling confidential or proprietary information	37%	22%
Breaching customer or consumer privacy	38%	16%
Falsifying or manipulating financial reporting information	32%	9%

Select Observations by Employees in Government and Regulatory Affairs Functions		
	2013	**2009**
Making false or misleading claims to the public or media	31%	19%
Providing inappropriate information to analysts or investors	23%	13%
Providing regulators with false or misleading information	20%	12%
Making improper political contributions to domestic officials	17%	7%
Doing business with third parties that may be involved in money laundering	9%	4%
Making improper payments or bribes to foreign officials	7%	3%

Select Observations by Employees in General Management and Administration Functions		
	2013	**2009**
Wasting, mismanaging, or abusing the organization's resources	42%	46%
Mishandling confidential or proprietary information	30%	26%
Engaging in activities that pose a conflict of interest	30%	23%
Stealing or misappropriating assets	28%	21%
Falsifying or manipulating financial reporting information	24%	12%

2.2 Understanding Acceptable Conduct

Familiarity with Policies, Laws, Regulations, Code, Values, and Principles

We asked respondents whether or not they understood the organizational values, standards, and policies that define acceptable business practices for their positions. We found high levels of familiarity with such standards – albeit slightly decreased from our 2009 survey results – as well as favorable views on the communication and training employees received related to those standards.

Employee Familiarity with Standards of Conduct		
	2013	**2009**
Specific policies, laws or regulations unique to my job function	78%	84%
My organization's code of conduct	77%	83%
My organization's overall values and principles	77%	82%

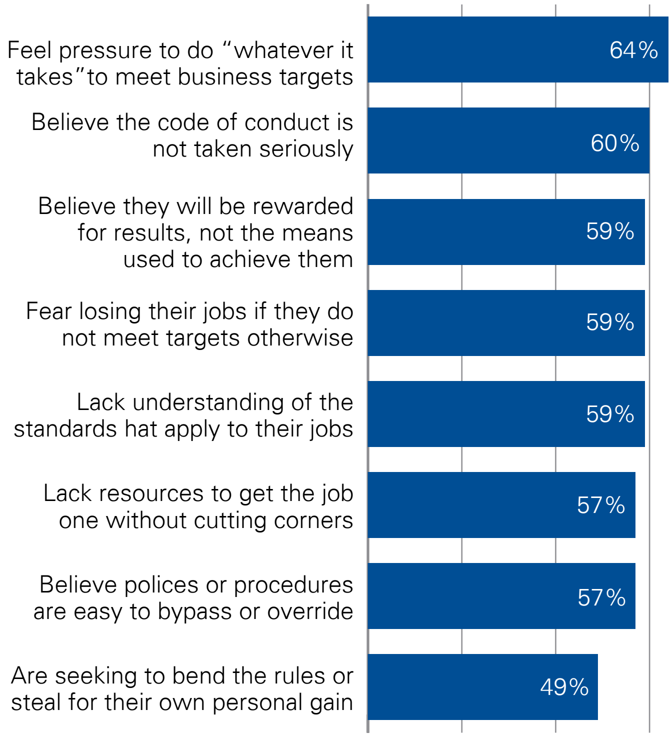
Organizations that take preventative measures to thwart misconduct through communication and training more frequently see their efforts succeed. More than 90 percent of respondents reported that the communication and training they received on the standards of conduct of their organization was clear, easy to understand, and available when needed. More importantly, greater than 90 percent of respondents also reported this training to be an effective tool in guiding individual decisions and behaviors at work.

Communication and Training Received On Standards of Conduct		
	2013	**2009**
Clear and easy for me to understand	93%	94%
Effective in guiding my decisions and behaviors at work	91%	91%
Provided to me when I need it	91%	90%

2.3 Preventing Misconduct

Efforts to prevent misconduct must take into account its root causes. Therefore, in addition to wanting to understand the prevalence and nature of misconduct in the workplace, we wanted to understand its root causes. And so we asked respondents what factors might cause managers and employees to engage in misconduct. As in previous surveys, the most commonly cited were pressure to meet targets; cynicism toward the organization's code of conduct; systems that rewarded results over means; and the fear of job loss if targets are not met.[1] Fewer respondents cited individual personal gain as a motivating factor for organizational misconduct.

Root Causes of Misconduct



2.4 Detecting Misconduct

Employees and managers are often in the best position to discover fraud and misconduct schemes. However, observing misconduct is one thing and having the confidence to report it is an entirely different thing. Therefore, we wanted to gauge the inclination of employees to report misconduct upon witnessing it, as well as their comfort level in raising concerns through various channels established by management for upward communication.

Propensity to Report Misconduct

We asked employees what they would do if they observed a violation of their organization's standards of conduct. The vast majority (78 percent) indicated that they would notify their supervisor or another manager and more than half (53 percent) said that they would call the ethics hotline (an increase from 44 percent in 2009 and 38 percent in 2005).

However, about a quarter of all participants said that they would look the other way or do nothing (23 percent, up from only 6 percent in 2009) or notify someone outside the organization (26 percent, up from only 10 percent in 2009). Such results demonstrate a continuing need for organizations to enhance the effectiveness of internal advice and reporting mechanisms, especially in light of the provisions of various Federal and state whistle blowing laws, including the recently enacted Dodd-Frank Act, which established a "bounty program" for whistleblowers who raise concerns directly with the Securities & Exchange Commission (note that whistleblowers are not required to report misconduct first within their organizations to qualify under the bounty program).

Propensity to Report Misconduct

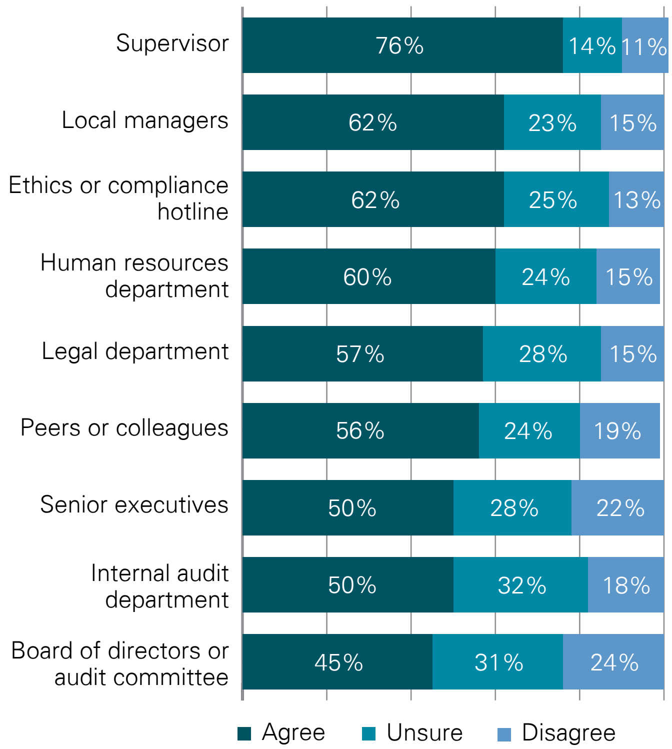
[1] See a comparison of this survey question's 2013 results with past survey results on page 17.

Channels for Reporting Misconduct

Next, we asked employees to whom they would turn or "feel comfortable" reporting misconduct if they suspected or became aware of it. As in previous surveys, supervisors and local managers led the responses to this question, which underscores the need for organizations to ensure that front-line managers and supervisors are well-prepared to respond appropriately to allegations.

Additionally, more than half of respondents said they would feel comfortable calling a hotline or turning to functions typically charged with responding to alleged misconduct (e.g., human resources or legal). Although about half of respondents said they would contact internal audit, senior executives, or the board or audit committee, these were among the least likely channels employees would feel comfortable using to report allegations. Finally, it is important to note a significant rise to 45 percent of respondents feeling comfortable turning to the board or audit committee, compared with our 2009 survey result of 32 percent.

Channels Employee "Feel Comfortable" Using to Report Misconduct



Channels for Seeking Advice and Counsel

In addition, we asked employees to whom they would turn to for advice and counsel if they had a question about "doing the right thing." Confidence levels in particular channels were generally on par with those for reporting misconduct, with a notable, characteristic rise in the selection of employee peers as a desirable channel for seeking advice.

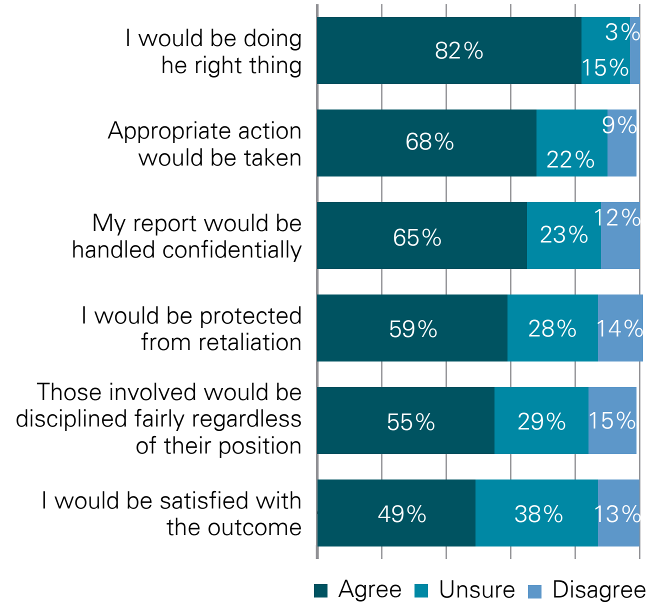
Channels Employee "Feel Comfortable" Using to for Advice and Counsel

2.5 Responding to Misconduct

Employee decisions about whether or not to report misconduct often correlate to their perceptions of the outcome of the report as well as the actions of their organization in response to allegations of misconduct. Therefore, we asked employees what they believed would happen if they reported an integrity breakdown to management.

While a majority of 82 percent acknowledged they would be "doing the right thing," nearly half were uncertain they would be protected from retaliation (based upon "unsure" and "disagree" responses). About a third of respondents lacked confidence that appropriate action would be taken or that the report would be handled confidentially. Finally, more than half suggested a lack of confidence that they would be satisfied with the outcome. These results suggest that organizations must rededicate their efforts in this area if they wish to keep employees raising concerns "in-house" rather than to regulators or law enforcement (e.g., under the whistleblower provisions of the Dodd-Frank Act).

Perceived Outcomes of Reporting Misconduct



2.6 Perceived Tone and Culture

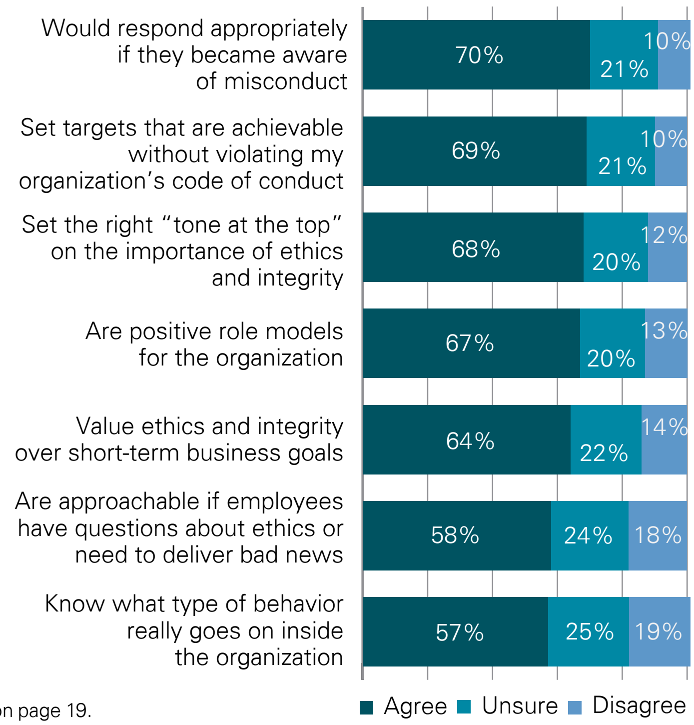
Tone at the Top

The "tone at the top" set by top leadership is often cited as a determining factor in creating organizational commitment to high ethics and integrity. As such, we sought to determine how employees perceived the tone at the top and character of the leadership within their own organizations.

We asked employees whether their chief executive officer and other senior executives exhibited characteristics attributable to personal integrity and ethical leadership. Approximately two-thirds of employees agreed that their leaders set the right tone regarding the importance of ethics and integrity and served as positive role models for their organizations, leaving one third unsure or in disagreement.

More than half of respondents believe that top leadership values ethics and integrity over short-term business goals, indicating an upward trend from our previous surveys.[2] Interestingly, almost half of employees surveyed believed that the top leaders within their organization were unaware of the behavior that exists throughout the organization.

Perceptions about the CEO and Other Senior Executives



[2] See a comparison of this survey question's 2013 results with past survey results on page 19.

Local Tone

Because the tone set by top leadership in larger organizations may have a limited reach and less influence upon those employees who are "in the trenches," we wanted to understand employees' perceptions of the tone set by local supervisors and managers. Our 2013 survey results showed little change from our 2009 results, with almost three quarters of respondents perceiving local managers and supervisors as approachable with questions or bad news, and capable of responding appropriately to misconduct. Seventy one percent of local managers and supervisors were also seen by employees as positive role models that set achievable targets and demonstrated an appropriate "local tone" on the importance of ethics and integrity.

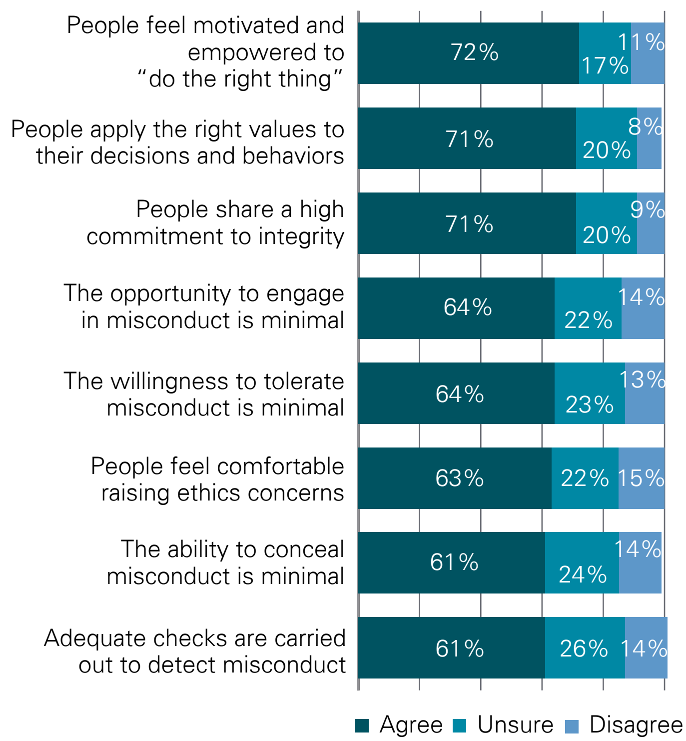
In comparison to the scores of top leadership on this topic, local managers and supervisors received more favorable results across the board, suggesting that employees' greater familiarity with local managers and supervisors corresponds to higher levels of trust and confidence.

Perceptions of Local Managers and Supervisors

Team Culture and Environment

It stands to reason that when the CEO's speech at the town hall meeting is over, employees are most influenced by their immediate teams and work units. Therefore, we asked employees nationally how they would characterize the team environment that immediately surrounds them. Results were generally favorable across many indicators, with approximately two thirds of employees believing that their individual teams and work units applied the right values to decisions and behaviors, possessed a high commitment to integrity, and felt motivated to do the right thing. In fact, employee perceptions of their individual teams scored favorable results of more than 60 percent across each indicator.

Perceptions of Individual Teams and Work Units



Comparison of Data Over Time

3

Prevalence of Misconduct

While the prevalence and seriousness of misconduct have remained consistent over the past decade, our 2013 results show an increase in the significance of misconduct being observed.

Prevalence of Misconduct				
% Employees Nationally	**2013**	**2009**	**2005**	**2000**
Observed misconduct in the prior 12-month period	73%	74%	74%	76%
Believed observations could cause "a significant loss of public trust if discovered"	56%	46%	50%	49%

Root Causes of Misconduct[3]

Perhaps not surprising given the current economic crisis we found thematic increases across the board in employee perceptions of the root causes of misconduct.

Root Causes of Misconduct				
% Employees Nationally	**2013**	**2009**	**2005**	**2000**
Feel pressure to do "whatever it takes" to meet business objectives	64%	59%	57%	65%
Believe they will be rewarded for results, not the means used to achieve them	59%	52%	49%	56%
Lack understanding of the standards that apply to their jobs	59%	51%	55%	50%
Believe their code of conduct is not taken seriously	60%	51%	52%	73%
Lack resources to get the job done without cutting corners	57%	50%	49%	70%
Fear losing their jobs if they do not meet targets otherwise	59%	49%	46%	*No data*
Believe polices or procedures are easy to bypass or override	57%	47%	47%	*No data*
Are seeking to bend the rules or steal for their own personal gain	49%	34%	33%	22%

[3] The precise wording of this series of questions was modified between 2000 and subsequent years. The data shown for 2000 corresponds to a similar, but different phrasing of questions than the ones posed in subsequent years (shown in this table). Therefore, the comparison with data from 2000 may be viewed as directional or thematic.

Propensity to Report Misconduct[4]

The propensity to report misconduct to a supervisor or another manager remained relatively consistent in our last three surveys. However, a thematic rise in the acceptance of an ethics or compliance hotline as a communication channel of choice is evident from year to year.

Perhaps in a nod to recent legislation such as the U.S. Dodd-Frank Act's whistleblower provisions, a significantly larger number of respondents said they would notify someone outside the organization if they observed misconduct. Finally, in a troubling upward trend, 23 percent of employees in 2013 said they would look the other way or do nothing if they encountered misconduct (up from only 6 percent in 2009).

Propensity to Report Misconduct				
% Employees Nationally	**2013**	**2009**	**2005**	**2000**
Notify supervisor or another manager	78%	81%	81%	63%
Try resolving the matter directly	54%	52%	53%	40%
Call the ethics or compliance hotline	53%	44%	38%	21%
Notify someone outside the organization	26%	10%	10%	4%
Look the other way or do nothing	23%	6%	6%	5%

Channels for Reporting Misconduct

Confidence in various channels for reporting misconduct increased between 2009 and 2013. For example, confidence in reporting misconduct through a hotline continued to climb between those years. Moreover, employees were also more confident in reporting misconduct to senior executives and board members, as well as to organizational functions with responsibility for responding to misconduct (e.g., human resources and legal).

Channels for Reporting Misconduct				
% Employees Nationally	**2013**	**2009**	**2005**	**2000**
Supervisor	76%	78%	78%	77%
Local managers	62%	61%	62%	*No Data*
Peers or colleagues	56%	57%	57%	*No Data*
Human resources department	60%	57%	56%	56%
Ethics or compliance hotline	62%	57%	53%	40%
Senior executives	50%	43%	44%	43%
Legal department	57%	52%	52%	40%
Internal audit department	50%	40%	39%	*No Data*
Board of directors or audit committee	45%	32%	32%	*No Data*

[4] The response scale for this question was modified in 2005 and subsequent years. The data shown for 2000 corresponds to a frequency scale (e.g., often, sometimes, never), whereas the data shown in subsequent years corresponds to an agreement scale (e.g., agree or disagree). Therefore, the comparison from our 2000 data may be viewed as directional or thematic.

Perceived Outcomes of Reporting Misconduct to Management

In virtually all criteria, employees expressed a continuing trend of greater confidence than they had in the past in the outcomes of reporting misconduct to management.

Perceived Outcomes of Reporting Misconduct				
% Employees Nationally	**2013**	**2009**	**2005**	**2000**
Appropriate action would be taken	68%	66%	67%	61%
My report would be handled confidentially	65%	64%	64%	59%
I would be protected from retaliation	59%	53%	52%	47%
Those involved would be disciplined fairly regardless of their position	55%	47%	47%	39%
I would be satisfied with the outcome	49%	39%	39%	*No Data*
I would be doing the right thing	82%	89%	89%	85%

Perceptions of the CEO and Other Senior Executives[5]

Employee perceptions of the CEO and other senior executives in 2013 generally remained consistent with our 2009 survey results. Note, however, there are significant increases in employee perceptions of senior executives' knowledge of behaviors within the organization, as well as their valuing ethics and integrity over short-term business goals.

Perceptions of the CEO and Other Senior Executives				
% Employees Nationally	**2013**	**2009**	**2005**	**2000**
Are positive role models for the organization	67%	64%	65%	60%
Know what type of behavior really goes on inside the organization	57%	49%	48%	43%
Are approachable if employees have questions about ethics or need to deliver bad news	58%	54%	55%	45%
Values ethics and integrity over short-term business goals	64%	56%	57%	*No Data*
Set targets that are achievable without violating my organization's standards of conduct	69%	67%	67%	58%
Would respond appropriately if they became aware of misconduct	70%	70%	70%	64%
Set the right "tone at the top" on the importance of ethics and integrity	68%	66%	65%	*No Data*

[5] The precise wording of this question was modified between 2000 and subsequent years. The 2000 data shown corresponds to a similar, yet different, question than the ones posed in subsequent years (shown in table). As such, the comparison from our 2000 data on this question may be viewed as directional or thematic.

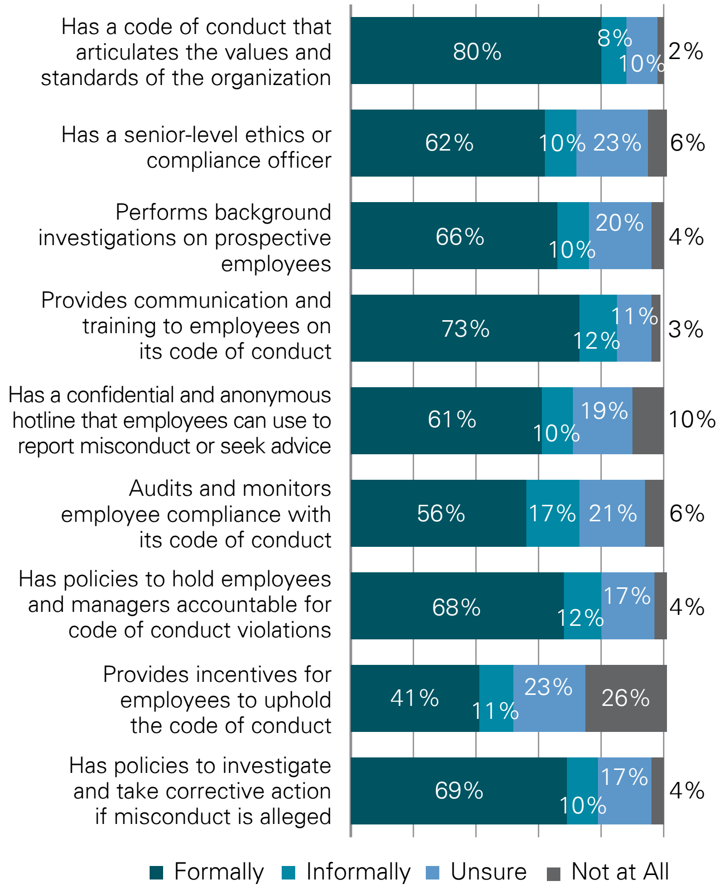
Influence of Ethics and Compliance Programs 4

4.1 Program Elements

Formal ethics and compliance programs are increasingly common. Such programs, also referred to as "antifraud programs and controls" in auditing standards and literature, have been largely reinforced by government legislation, regulatory guidance, and enforcement policies as outlined later in this report. And yet, the presence of an ethics and compliance program does not guarantee an organization's commitment to it. Therefore we wanted to gauge whether or not specific program elements were recognizable to employees, and to understand whether or not the presence of various program elements influence the indicators measured in the survey.

We asked employees whether or not their organizations had specific ethics and compliance program elements as shown in the table below. While our 2013 survey results generally remained consistent with the 2009 results, we did note a significant increase of organizations providing incentives for employees to uphold the code (41 percent in 2013 as compared to 26 percent in 2009) and in auditing and monitoring employee compliance with the code (56 percent in 2013 as compared to 49 percent in 2009).

Presence of Program Elements



May not add to 100 percent due to rounding.

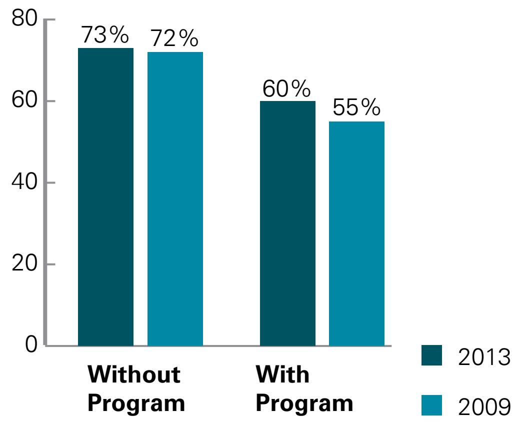
4.2 Correlation

Next, we wanted to correlate the presence of ethics and compliance program elements to the behaviors and perceptions measured elsewhere in the survey. To do so, we split respondents into two groups– the first group representing employees who classified themselves as working in organizations with a comprehensive ethics and compliance program, the second group representing employees who did *not* classify themselves this way. For shorthand, we refer to these groups as "with program" and "without program" in the analysis that follows.[6]

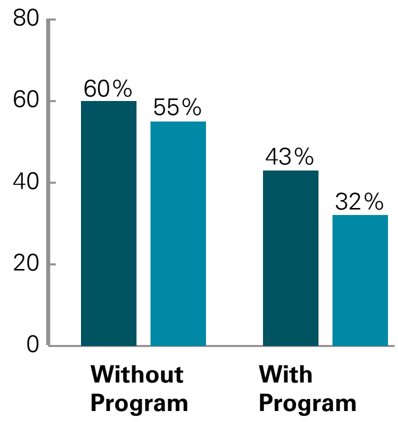
Prevalence of Misconduct
While ethics and compliance programs continue to have a favorable influence on the prevalence of misconduct, we do note in 2013 a higher number across the board of employees who observed violations of organizational values and principles.

Root Causes of Misconduct
While we note in 2013 significant increases in employee perceptions of the root causes of misconduct regardless of whether or not a compliance program was in place, such programs continue to have a favorable influence on factors that contribute to misconduct. For example, of those respondents who worked in organizations that *did not* have a compliance program, a higher number of employees in 2013 felt pressure to do whatever it takes to meet performance targets.

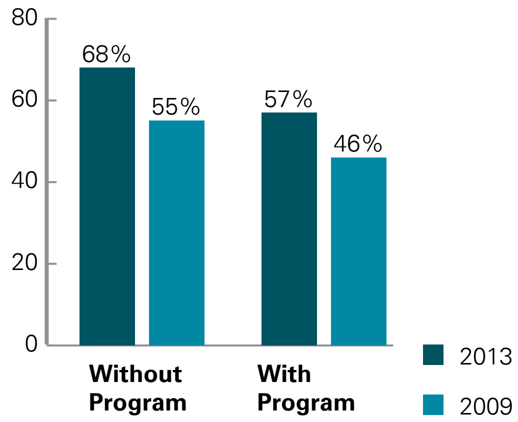
Observed misconduct (all) in the prior 12 months



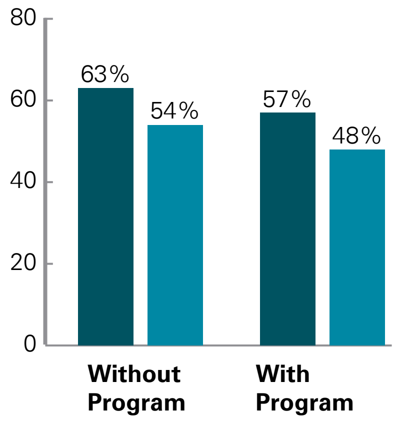
Observed violations of organizational values and principles in the prior 12 months



Feel pressure to do whatever it takes to meet targets

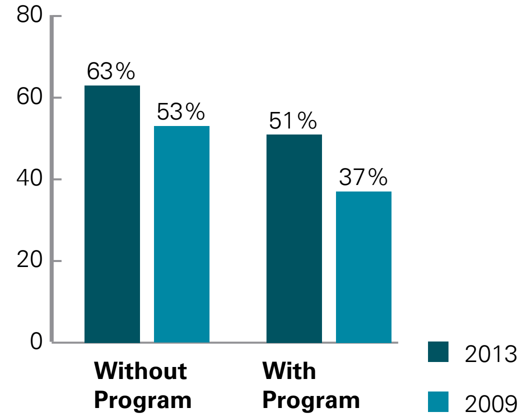


Lack understanding of standards that apply to their job

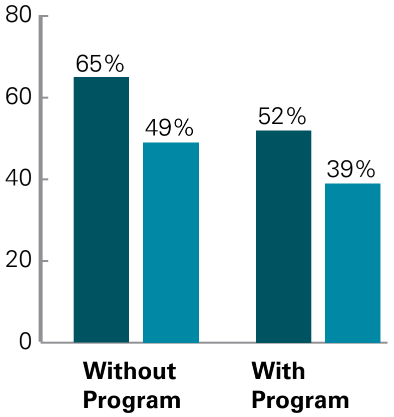


[6] The "with program" group represents employees who indicated that their organizations had "formally" implemented all program elements included in the survey. The "without program" group represents those employees who did not classify themselves as working in organizations with a comprehensive ethics and compliance program. These represent employees who indicated they were "unsure" or who answered "not at all" when asked whether their organizations had implemented all program elements included in the survey. Employees who indicated that their organizations had only "informal" program elements were not included in our correlation analysis, which means the results presented in this section reflect a subset of the total population reflected in the previous section of the report.

Believe policies and procedures are easy to bypass or override



Believe rewards are based on results, not the means used to achieve them

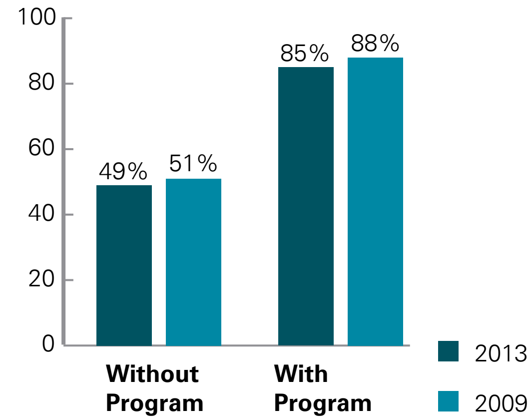


Detecting Misconduct

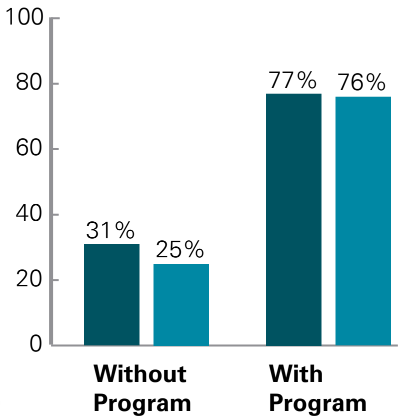
Channels for Reporting Misconduct

Ethics and compliance programs have a favorable affect upon employee willingness to report misconduct.

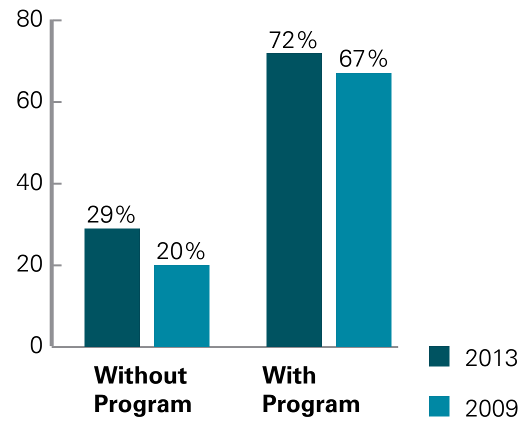
Would feel comfortable reporting misconduct to a supervisor



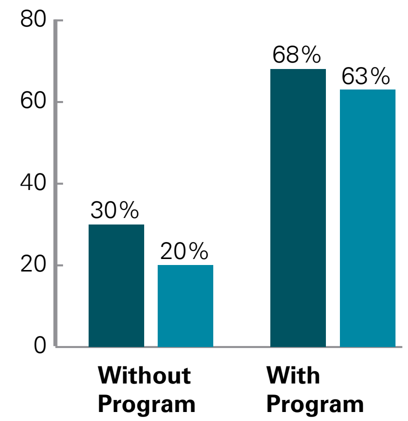
Would feel comfortable reporting misconduct to legal department



Would feel comfortable reporting misconduct to internal audit



Would feel comfortable reporting misconduct to board of directors

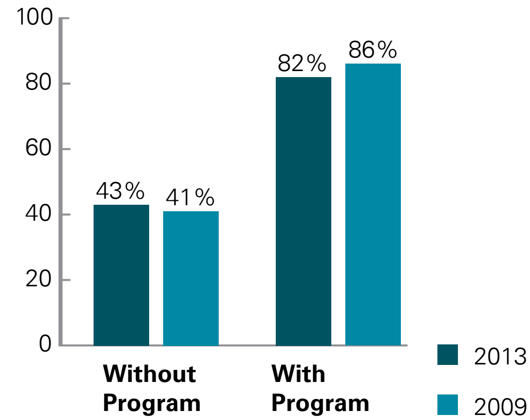


Responding to Misconduct

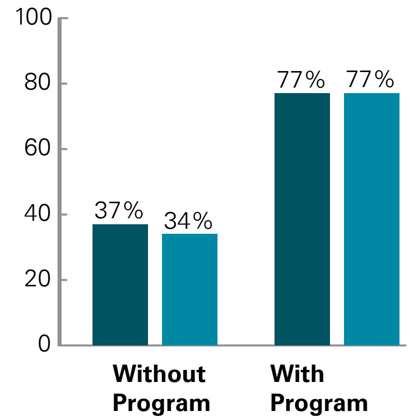
Perceived Outcomes of Reporting Misconduct

The existence of ethics and compliance programs has a favorable effect upon employee perceptions of the outcomes of reporting misconduct. This is illustrated by our 2013 data that shows that of those employees working in an organization that *did not* have a compliance program, a significantly lower number of respondents believed "they would be doing the right thing" if they reported misconduct.

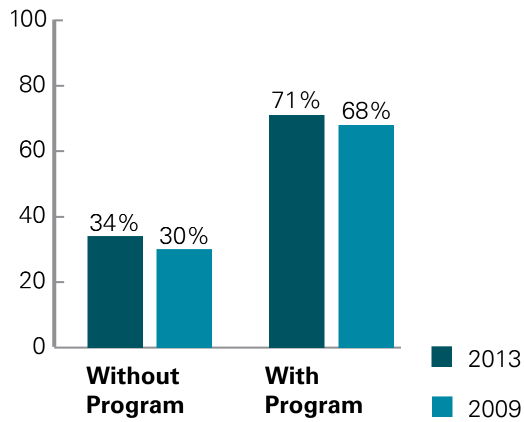
Believe appropriate action would be taken



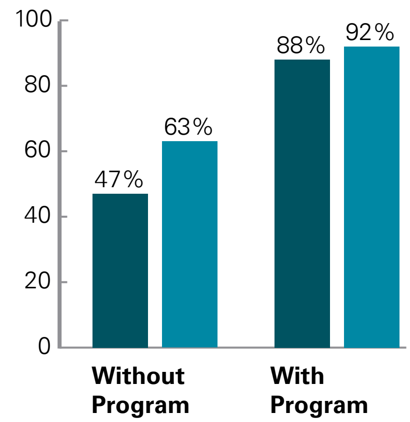
Believe they would be protected from retaliation



Believe they would be satisfied with the outcome



Believe they would be doing the right thing

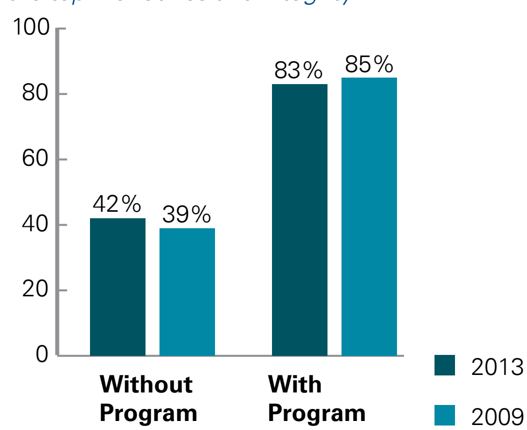


Tone and Culture

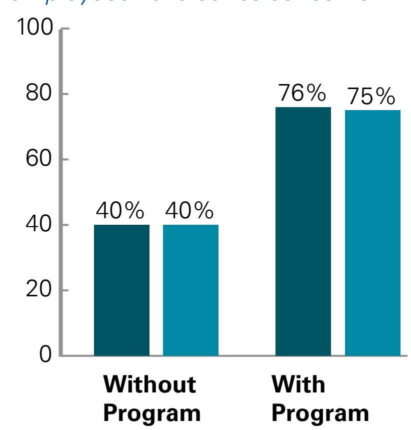
Tone at the Top

Ethics and compliance programs continue to have a favorable affect upon employee perceptions of the tone at the top.

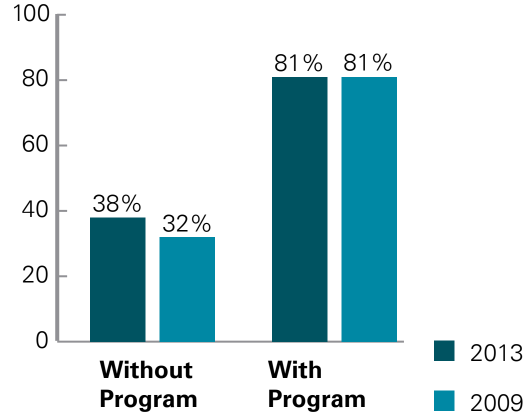
Believe CEO and other senior executives set the right "tone at the top" for ethics and integrity



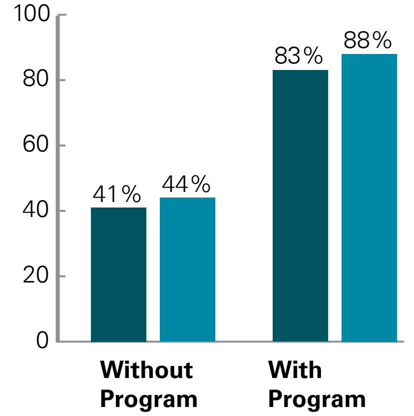
Believe CEO and other senior executives are approachable if employees have ethics concerns



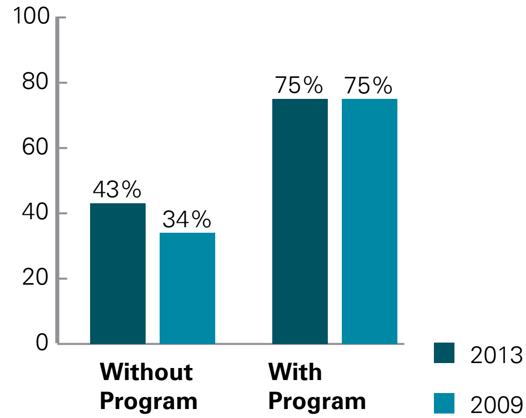
Believe CEO and other senior executives value ethics and integrity over short-term business goals



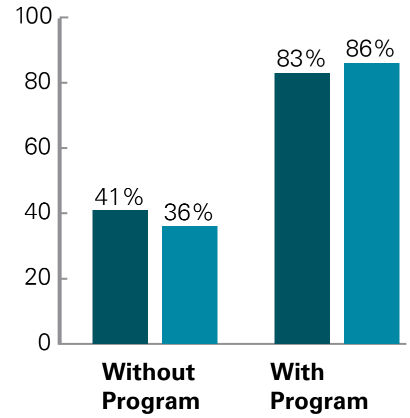
Believe CEO and other senior executives would respond appropriately if they became aware of misconduct



Believe CEO and other senior executives know what type of behavior goes on within the organization



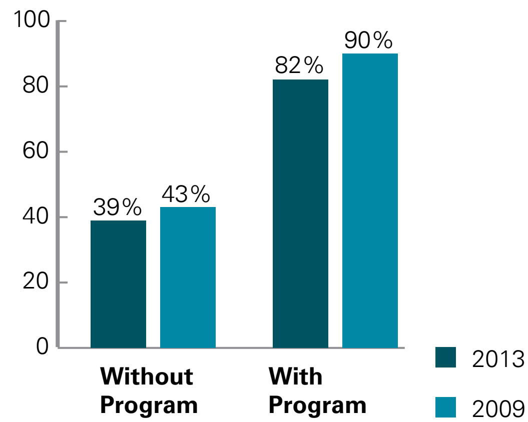
Believe CEO and other senior executives set targets that are achievable without violating the code of conduct



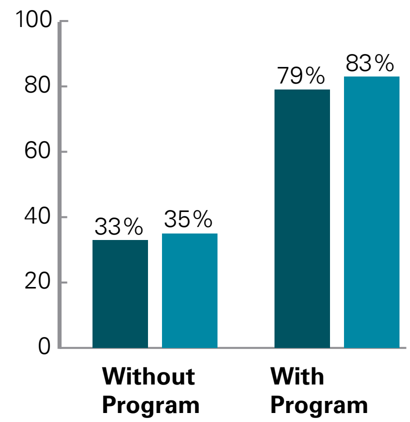
Team Culture and Environment

Ethics and compliance programs continue to have a favorable affect upon team culture and environment.

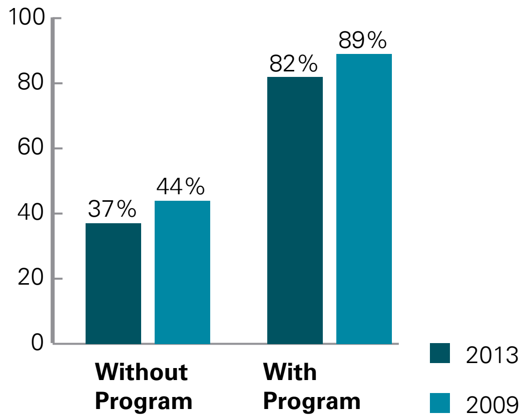
People feel motivated and empowered to "do the right thing"



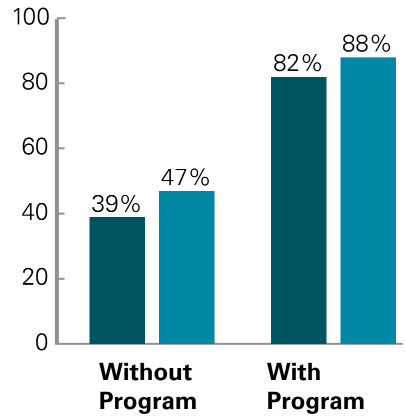
People feel comfortable raising and addressing ethics concerns



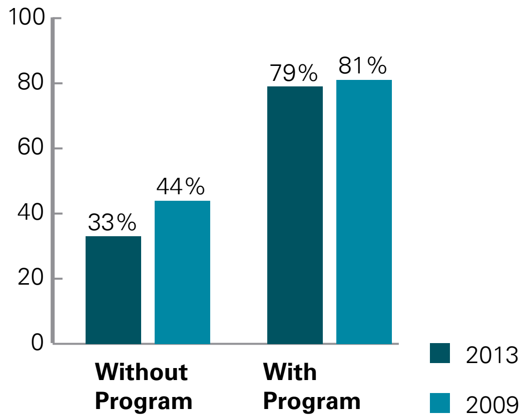
People apply the right values to their decisions and behaviors



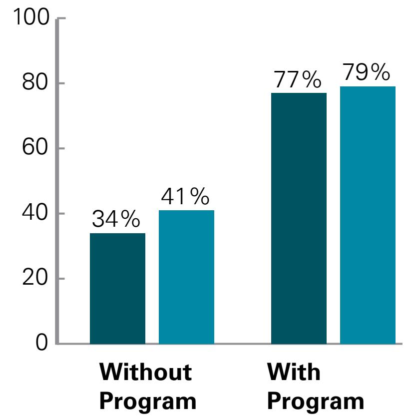
People share a high commitment to integrity



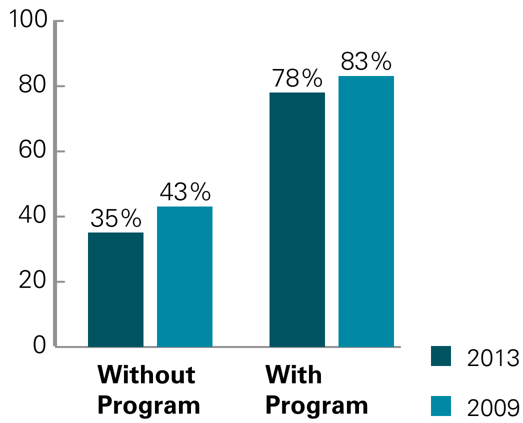
The opportunity to engage in misconduct is minimal



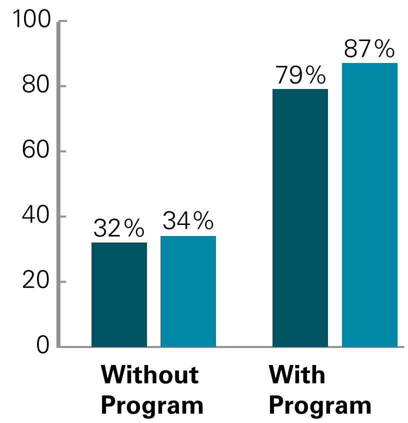
The ability to conceal misconduct is minimal



Willingness to tolerate misconduct is minimal



Adequate checks are carried out to detect misconduct



·Innovation
★ Professionalism
·Productivity
•EXECUTE
·Logistics
·Sustainability

Taking Action

5

Building a high-integrity organizational culture is a critical and ambitious undertaking and takes teamwork and dialogue. However, it is difficult to decide just where to begin the discussion. To help, this section offers some sample questions that boards and managers may wish to consider when taking stock of their own challenges and approaches to managing the risk of fraud and misconduct.

5.1 Covering the Basics

At the highest level, teams may wish to begin a conversation by asking…

- What controls do we have in place to prevent fraud and misconduct from occurring in the first place?
- What controls do we have in place to detect wrongdoing when it does occur?
- What controls do we have in place to respond appropriately to allegations or concerns when they arise?

Once key controls have been identified, teams may wish to consider…

- Have our controls been tailored based on an assessment of the types of fraud and misconduct risks that are likely to arise in the business today?
- Have our controls been designed in a manner consistent with minimum legal and regulatory criteria as well as industry practices that companies have generally found to be effective?
- Have our controls been implemented by functions with requisite levels of objectivity, competence, authority, and resources?
- Have our controls been recently evaluated to ensure that they are operating effectively?

5.2 Advancing the Conversation

Directors and managers looking to enhance the quality of organizational discussions regarding the effectiveness of risks and controls may wish to inquire how the organization is addressing emerging challenges such as the following:

Prevention Considerations

- Does our ethics and compliance program target the underlying pressures, rationalizations, and opportunities faced by managers and employees to engage in misconduct?
- How can we use case studies to educate our people on the risks that can come up in the business and the values that should inform their actions when dilemmas arise?
- Do our communication and training programs maintain relevance when delivered overseas, or are they too U.S.-centric?
- Are we performing the right level of due diligence on employees and third parties operating on our behalf internationally?
- Do we have the insights we need on the behavioral style of employees being promoted or transferred into positions of discretionary authority?
- Do our performance evaluations bring about a balanced examination of business results and the means used to achieve them?
- Is our program poised to anticipate and react to new ethics and compliance risks, or is it backward-looking and "fighting the last war"?

Detection Considerations

- Are concerns that get raised through non-hotline channels getting to the right place?
- Do we leverage feedback from alternative sources, such as customer complaints or employee exit interviews?
- Are fraud analytics embedded in our computer-based auditing and monitoring systems to detect suspicious events or transactions?
- Have our data analytic routines been expanded to address international risk areas, such as bribery and corruption?

Response Considerations

- Have we equipped front-line supervisors with the knowledge and tools to address allegations and concerns in an appropriate manner?
- Is there a uniform understanding across the business of what allegations require investigation, by whom, when, and in what manner?
- What factors should guide whether we hold managers accountable for wrongdoing by subordinates?
- Who should be involved in a decision to voluntarily disclose potential compliance violations to the government?

Board and Management Oversight Considerations

- Do the audit and compensation committees discuss how to address fraud and misconduct risks that may arise from executive compensation plans?
- Do management actions (e.g., annual goal setting, strategic planning, budgeting, resource allocation, and incentive compensation) align with the goals of our ethics and compliance program, or do they send mixed messages?
- Do stewards of the ethics and compliance program have the requisite levels of authority, stature, objectivity, and competence to do the job effectively?
- Have we positioned fraud risk management as a discipline that is embedded throughout the business or as a disconnected department?

Evaluation Considerations

- What metrics and key performance indicators should we use to monitor the effectiveness of our program? Are employee perceptions and attitudes toward our program among the indicators we formally track?
- What information do we share with line managers and employees to foster understanding and confidence in our program?
- How do we demonstrate good governance and corporate social responsibility to external stakeholders?
- Do we define success for ethics and compliance programs purely from a risk-avoidance perspective, or have we identified ways the program can accrue benefits to the brand and our bottom line?

Meeting the Regulatory Challenge 6

The Federal government has responded to corporate scandals and fraudulent activity by instituting legislative and regulatory reforms that encourage companies to become more self-governing.

The establishment of an effective ethics and compliance program and related antifraud programs and controls is a common denominator across numerous legislative and judicial policies, and the cornerstone of an effective corporate fraud risk management strategy.

6.1 Sarbanes-Oxley Act of 2002 (Section 404)

Section 404 of the Sarbanes-Oxley Act requires companies and their auditors to evaluate the effectiveness of their internal controls over financial reporting based on a suitable control framework. Most companies in the United States are applying the integrated internal control framework developed by the Committee of Sponsoring Organizations ("COSO"). Generally speaking, the COSO framework addresses compliance program elements in entity-wide components that have a pervasive influence on organizational behavior, such as the control environment.

Examples include:

- Establishment of the tone at the top by the board and management
- Existence of codes of conduct and other policies regarding acceptable business practices
- Extent to which employees are made aware of management's expectations
- Pressure to meet unrealistic or short-term performance targets
- Management's attitude toward overriding established controls
- Extent to which adherence to the code of conduct is a criterion in performance appraisals
- Extent to which management monitors whether internal control systems are working
- Establishment of channels for people to report suspected improprieties and
- Appropriateness of remedial action taken in response to violations of the code of conduct.

6.2 Corporate Governance Listing Standards

In response to provisions of the Sarbanes-Oxley Act, both the NYSE and NASDAQ adopted new corporate governance rules for listed companies. While the specific rules for each exchange differ, each includes standards that require listed companies to adopt and disclose codes of conduct for directors, officers, and employees and to disclose any code of conduct waivers for directors or executive officers. In addition, the rules of each exchange require listed companies to adopt mechanisms to enforce the codes of conduct.

6.3 U.S. Federal Sentencing Guidelines for Organizational Defendants

The Federal Sentencing Guidelines for Organizational Defendants, promulgated in 1991 by the United States Sentencing Commission, establish minimum compliance and ethics program requirements for organizations seeking to mitigate penalties for corporate crimes. Amended in 2004 and again in 2010, the Guidelines make it explicit that organizations are expected to promote a culture of ethical conduct, tailor each program element based on compliance risk, and periodically evaluate program effectiveness. Specifically, the amended Guidelines call on organizations to:

- Promote a culture that encourages ethical conduct and a commitment to compliance with the law
- Establish standards and procedures to prevent and detect criminal conduct
- Ensure the board of directors and senior executives are knowledgeable and exercise reasonable oversight over the compliance and ethics program
- Assign a high-level individual within the organization to ensure the organization has an effective compliance and ethics program and delegate day-to-day operational responsibility to individuals with adequate resources and authority and direct access to the board

- Ensure high-level individuals and those with substantial discretionary authority are knowledgeable about the program, exercise due diligence in performing their duties, and promote a culture that encourages ethical conduct and a commitment to compliance with the law
- Use reasonable efforts and exercise due diligence to exclude from positions of substantial authority individuals who have engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program
- Conduct effective training programs for directors, officers, employees, and other agents and provide such individuals with periodic information appropriate to their respective roles and responsibilities relative to the compliance and ethics program
- Ensure that the compliance and ethics program is followed, including monitoring and auditing to detect criminal conduct
- Publicize a system, which may include mechanisms for anonymity and confidentiality, through which the organization's employees and agents may report or seek guidance regarding potential or actual misconduct without fear of retaliation
- Evaluate periodically the effectiveness of the compliance and ethics program
- Promote and enforce the compliance and ethics program consistently through incentives and disciplinary measures and
- Take reasonable steps to respond appropriately to misconduct, including making necessary modifications to the compliance and ethics program.

6.4 The Dodd-Frank Wall Street Reform and Consumer Protection Law

The Dodd-Frank Act was enacted to ensure stability in the U.S. financial markets, affecting all U.S. financial institutions, many non-U.S. financial institutions, and many non-financial companies. The Act alters practices in banking, securities, derivatives, executive compensation, consumer protection, and corporate governance. Among others, the Act establishes a "bounty program" for whistleblowers who raise concerns with the U.S. Securities & Exchange Commission (SEC). The SEC has adopted a final rule to implement the Act's whistleblower award provisions, permitting individuals who provide the SEC with high-quality tips that lead to successful enforcement actions to receive a portion of the SEC's monetary sanctions while attempting to discourage them from side-stepping their company's internal reporting systems.

To be considered for an award, a whistleblower must voluntarily provide the SEC with original information that leads to the SEC's successful enforcement action with monetary sanctions greater than $1 million. An individual whistleblower may be eligible for an award of 10 percent to 30 percent of the monetary sanctions. The final rule, with some exceptions, excludes from eligibility original information obtained by a person with legal, compliance, audit, supervisory, or governance responsibilities for an entity, such as an officer, director, or partner, or if the information was communicated to the whistleblower through the company's internal compliance mechanisms, as well as information gained by an independent public accountant through the performance of an engagement (such as a financial audit) that is required under the securities laws.

The final rule does not necessarily render a whistleblower ineligible to receive an award if the whistleblower engaged in the same fraud or misconduct that he or she is reporting. Instead, the SEC will consider the nature and severity of the misconduct to determine if the whistleblower may collect an award. The SEC responded to concerns that its whistleblower award program, as originally proposed, might negatively affect a company's internal ethics and compliance processes by providing incentives for a whistleblower to participate in a company's internal compliance and reporting system. However, the rule does not require a whistleblower to report violations of securities laws internally to qualify for an award under the SEC's program.

In determining the amount of an award, voluntary participation in a corporate internal compliance and reporting system may increase the reward while interference with a corporate internal reporting program may reduce the reward. Moreover, the final rule provides that if a whistleblower reports information through the employer's internal compliance and reporting system, and the company subsequently self-reports to the SEC, the whistleblower is credited with the report and is eligible for any resulting award.

6.5 Department of Justice Prosecution Policy

In August 2008, the U.S. Department of Justice amended its guidelines related to the federal prosecution of business organizations in cases involving corporate wrongdoing. While the guidance states that a compliance program does not absolve a corporation from criminal liability, it does provide factors that prosecutors should consider in determining whether to charge an organization or only its employees and agents with a crime.

These factors include evaluating whether:

- The compliance program is merely a "paper program" or has been designed and implemented in an effective manner
- Corporate management is enforcing the program or tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives
- The corporation has provided for a staff sufficient to audit and evaluate the results of the corporation's compliance efforts
- The corporation's employees are informed about the compliance program and are convinced of the corporation's commitment to it.

6.6 Director and Officer Liability

An influential Delaware court broke ground in 1996 with its *In re Caremark Int'l Inc. Derivative Lit.* decision. The *Caremark* case was a derivative shareholder action brought against the board of directors of Caremark International alleging directors breached their fiduciary duties by failing to monitor effectively the conduct of company employees who violated various state and federal laws—which led to the company's plea of guilty to criminal charges and payment of substantial criminal and civil fines.

The court held that boards of directors that exercise reasonable oversight of a compliance program may be eligible for protection from personal liability in shareholder civil suits resulting from employee misconduct. The *Caremark* case pointed out that the compliance program should provide "timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with laws and its business performance." It also made clear that a director's fiduciary duty goes beyond ensuring that a compliance program exists, but also that "[t]he director's obligation [also] includes a duty to attempt in good faith to assure that [the compliance program] is adequate…."

Ten years later, the Delaware Supreme Court affirmed the *Caremark* standard for director duty in *Stone v. Ritter*, 911 A.2d 362 (Del. 2006), opining that "Caremark articulates the necessary conditions for assessing director oversight liability" and that the standard is whether there is a "sustained or systematic failure of the board to exercise oversight—such as an utter failure to attempt to assure a reasonable [compliance program] exists…"

Background and Methodology

7

As in previous surveys, we set out to understand the prevalence and nature of corporate fraud and misconduct in the U.S., along with the effectiveness of management efforts to prevent, detect, and respond appropriately to wrongdoing. To do so, we conducted a blind, national survey of pre-screened working adults that fell into demographic categories spanning six levels of job responsibility, 16 job functions, 13 industry sectors, and 5 thresholds of organizational size.

The overall methodology and tools for the survey were developed by KPMG professionals with substantial subject matter knowledge and experience relevant to conducting a study of this nature.

KPMG retained Walker Information, an independent survey research firm, to validate the manner in which questions were posed in the questionnaire; develop sample sizes across demographics categories established by KPMG; tabulate survey responses; and test the statistical validity of the survey's findings.

Walker Information, in turn, retained EMI-Online Research Solutions, a national panel database firm, to administer the survey to pre-screened members of its panel that met certain demographic criteria based on industry sector and organizational size. Individual respondents to the survey received nominal payment or consideration from EMI-Online Research Solutions for their participation. KPMG was not identified to the participants as being associated with the survey. Similarly, the names of the participants were not provided to Walker Information or KPMG.

Overall Sample

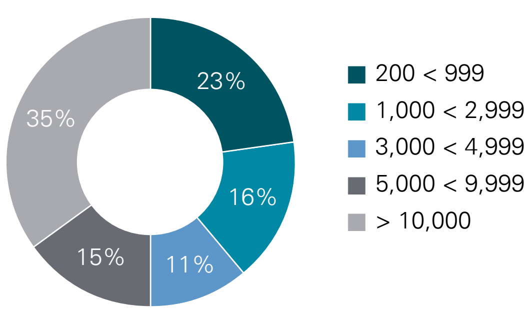
Total respondents	3573
Confidence level	95%
Precision level (margin of error)	+/-1.64%

7.1 Respondent Demographics

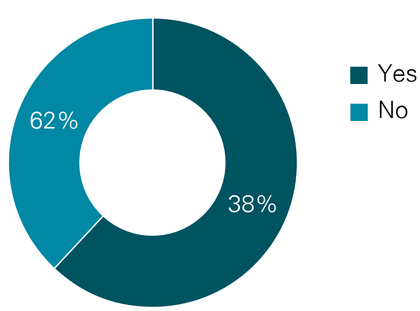
Respondents' Industry Classification

Aerospace & Defense	5%	Government & Public Sector	11%
Automotive	10%	Healthcare	10%
Banking & Finance	11%	Insurance	10%
Consumer Markets	9%	Media & Communications	3%
Chemicals & Diversified Industrials	5%	Pharmaceuticals & Life Sciences	3%
Electronics, Software & Services	9%	Real Estate & Construction	10%
Energy & Natural Resources	5%		

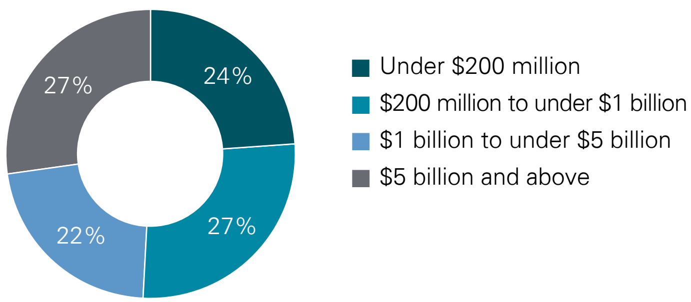
Respondents' Organizational Size (Total Number of Employees)



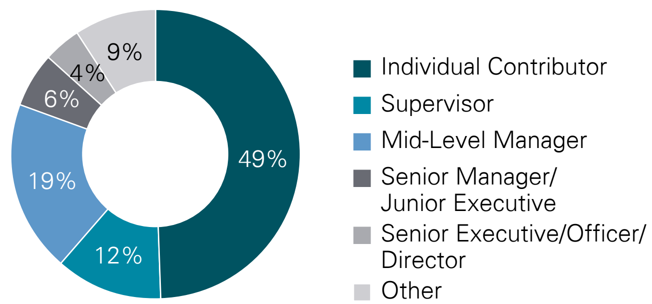
Respondent Conducting Business Internationally?



Respondents' Organizational Revenue



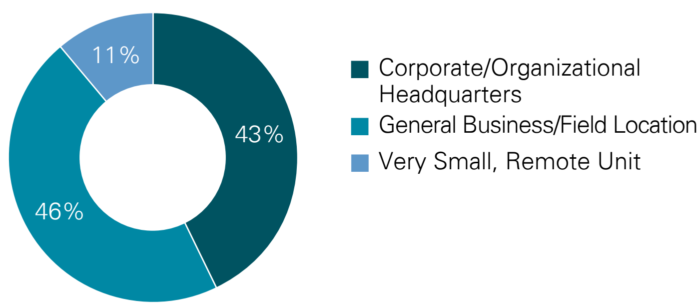
Respondents' Level of Responsibility



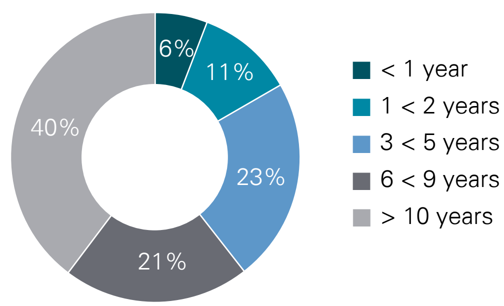
Respondents' Job Function

Sales/Marketing	9%	Clerical/Support	9%
Operations/Service	12%	General Management/Administration	9%
Manufacturing/Production	7%	Finance/Accounting	7%
Research/Development/Engineering	10%	Legal/Compliance	1%
Purchasing/Procurement	2%	Internal Audit/Risk Management	1%
Technology	12%	Public/Media Relations	1%
Training/Education	2%	Government/Regulatory Affairs	3%
Quality/Safety/Environmental	3%	Other	12%

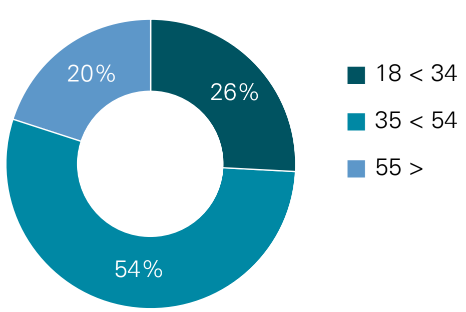
Respondents' Work Location



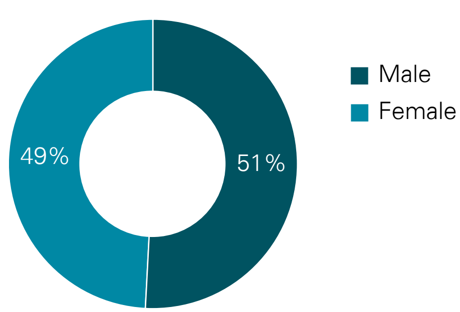
Respondents' Job Tenure



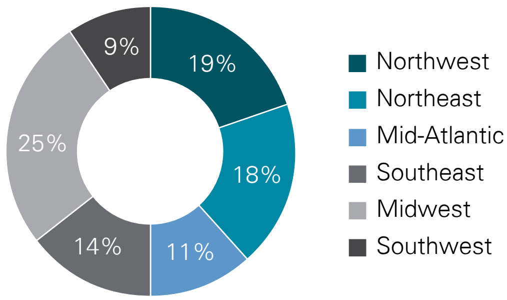
Respondents' Age



Respondents' Gender



Respondents' Geography (U.S.)



May not add to 100 percent due to rounding.

7.2 Frequently Asked Questions

Q. **How can I determine if employees from a particular company were among the participants in the survey?**

This was a blind survey. KPMG was not identified to the participants as being associated with the survey, and neither the names of participants nor the names of their employers were provided to KPMG.

Q. **How were participants for the survey selected?**

A panel database firm was retained to identify participants who: (i) were U.S. working adults; (ii) worked for organizations that employed at least 200 people; and (iii) worked for organizations in one of 13 broad industry sectors identified by KPMG.

Q. **Would it be correct to say that the results of this survey are reflective of the overall U.S. population?**

No. Employees in our sample population work for organizations that employ at least 200 employees. On average, most employees in the U.S. work for organizations that employ fewer numbers of people.

Q. **Does KPMG make its questionnaire and other detailed data publicly available?**

Not typically. All questions and data associated with this survey are proprietary to KPMG. While it is our practice to share high-level results of our national benchmarking study publicly, our primary objective in this research goes to supporting our clients in applying the survey within their own organizations. Therefore, additional tools related to this survey are typically only shared with clients who have specifically contracted for their use. We do occasionally share information with certain institutions for authorized academic research purposes.

About KPMG Forensic

8

KPMG Forensic is a global practice comprising multidisciplinary professionals from KPMG member firms who can assist clients in their efforts to achieve the highest levels of business integrity through the prevention, detection, and investigation of fraud and misconduct. This practice not only helps clients discover the facts underlying concerns about fraud and misconduct but also assists clients in assessing their vulnerabilities to such activities and in developing controls and programs to assess those risks.

KPMG Forensic uses computer forensic and data analysis techniques to help clients detect potentially fraudulent activity and other forms of misconduct. In addition, KPMG LLP, the U.S. member firm, operates the Cypress Technology Center ("CTEC"), which offers sophisticated technology tools and skilled professionals to help clients reduce litigation costs and risks in the areas of evidence and discovery management and the acquisition, management, and analysis of large data sets.

Professionals in the KPMG Forensic practice draw on experience in forensic accounting, law enforcement, fraud and misconduct risk assessment, antifraud risk controls, program design and implementation, asset tracing, computer forensics, and forensic data analysis.

Through KPMG's network of member firms, with professionals from the Americas, Asia Pacific, and Europe to the Middle East and Africa, KPMG Forensic practices are well positioned to provide consistent service to global clients. KPMG can readily assemble multinational teams comprising members who have shared methodologies, demonstrated technical skills, and deep industry knowledge.

Key Contacts

9

Richard H. Girgenti
National Practice Leader, KPMG Forensic
KPMG LLP in the United States
rgirgenti@kpmg.com
212-872-6953

Tim Hedley
Partner and Global Lead, Fraud Risk Management Services
KPMG LLP in the United States
thedley@kpmg.com
212-872-3496

9.1 Acknowledgements

KPMG wishes to thank the following individuals and organizations for their assistance in producing this survey:

- Ori Ben-Chorin, Director, KPMG Forensic
- Chris Woolard, Walker Information
- Mark Boston, Walker Information
- EMI-Online Research Solutions

kpmg.com