10 Principles of Legal and Compliance Risk Management



Gartner®

Principles of Risk Management

Legal and compliance departments routinely rank risk management as a top priority and a core department mandate. This is no surprise. In large part, both departments' value derives from the ability to help the business achieve strategic objectives while managing exposures to legal and regulatory risk, reputational damage and asset loss.

While aspects of risk management are different across companies, there are general principles that legal and compliance should follow. Based on over 15 years of research, this report lists 10 core principles of risk management for general counsels and chief compliance officers.

Risk Management Principles



Align Risk Management With Business Strategy

Legal and compliance must enable the business to take appropriate risks in pursuit of its objectives with a full view into accuracy of risk assessment and cost of mitigation.

- Principle 1: Align Risk Management to Company Strategy
- Principle 2: Build Your Legal and Compliance Risk Intelligence



Drive Decision Making

Risk management is valuable to the extent it better illustrates the nature and costs of risks and drives appropriate, consistent risk-taking behavior (e.g., employees operate within established risk tolerance).

- Principle 3: Conduct Activity-Based Assessments
- Principle 4: Monitor Risk Drivers
- Principle 5: Contextualize Business Decisions



Reduce Cost of Risk Mitigation

True risk management considers the overall cost of risk mitigation and strives to reduce it to the lowest necessary levels.

- Principle 6: Embed Risk Discipline in Operations
- Principle 7: Align Assurance Efforts



Build a Risk-Addressing Culture

Legal and compliance should build a strong risk culture that addresses the behavioral roots of unwanted risk creation.

- Principle 8: Create a Culture of Integrity
- Principle 9: Support Local Climate
- Principle 10: Improve Information Flows

Source: CEB, now Gartner analysis.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner®

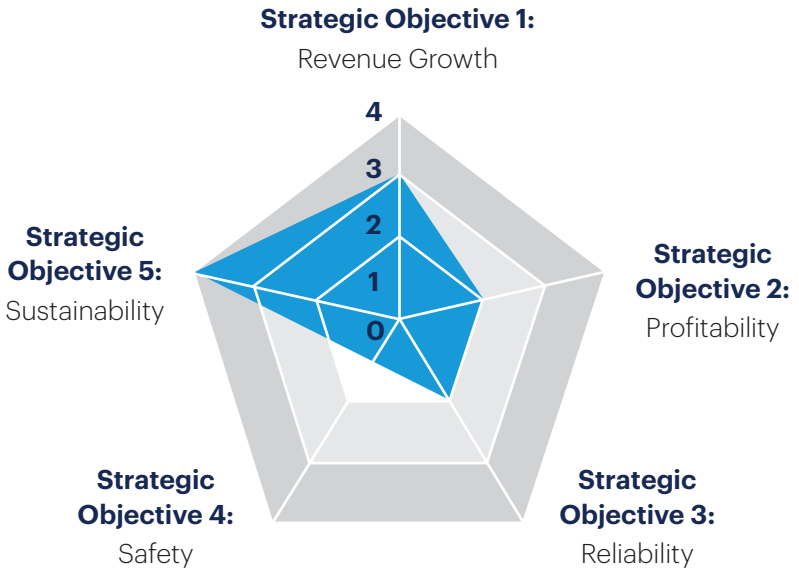
Principle 1

Align Risk Management to Company Strategy

True risk management means pursuing a correct level of risk, one that considers the goals of the firm and the cost of mitigation.

To meaningfully manage risks, legal and compliance must understand the level of risk and the trade-offs the company is willing to make in pursuit of its objectives.

Risk Appetite Plot for Strategic Objectives



By defining a risk appetite for each of their strategic objectives, companies can clarify decision making around each strategic priority. This further enhances the actionability of the risk appetite guidance.

Key Questions

- **Tolerance for Uncertainty:** How willing are you to accept uncertain outcomes?
- **Choice:** When faced with multiple options, how willing are you to select an option that puts this objective at risk?
- **Trade-Off:** How willing are you to trade off this objective against achievement of other objectives?
- **Practical Risk Appetite:** How does the tolerance for legal and compliance risks impact the legal authorizations, policies, templates, tools and playbooks that govern decisions?

Source: CEB, now Gartner analysis.
Note: Scores represent consensus view of risk appetite for reach strategic objective, represented on each axis.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner®

Principle 2

Build Legal and Compliance Risk

Risk management is an exercise in defining uncertainty. The best risk managers define core risks for which the company is "paid" and non core risks for which the company has no need or expertise.

For legal and compliance, this means building deep risk management expertise (an information advantage) where it is core to strategic success.

Risk Intelligence Decision Matrix



What to Keep In-House

The company should devote legal and compliance resources to manage and more accurately assess risks within activities that differentiate it from competitors and build competitive advantage.

Source: CEB, now Gartner analysis.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner®

Principle 3

Conduct Activity-Based Risk Assessment

Most risk assessments consider risks separate from their specific business context.

The result is often vague risk reports that don't capture the business context that most affects the risk.

Vista's[1] Risk and Control Assessment

Illustrative

Activity-Based Filters

Filter results by activity to identify the business touchpoints that contribute the most to overall risk exposure.

Operational Root Causes

Risk rating of the specific business activity creates more precise, targeted mitigation.

Risk	Activity	Inherent Risk[a]	Control Effectiveness Scale of 1 to 3	Residual Risk[b]	Risk- Specific Weight	Overall Compliance Risk Weight
Data Privacy	Promotional Interactions With Patients	15	1	15	60%	28%
	Market Research	12	2	6	24%	11%
Antitrust, Unfair Competition and Competitor Disparagement	Promotional Interactions With Patients	20	2	10	63%	19%
	Hospital Sponsorships	18	3	6	38%	11%
Corruption and Bribery	Education Grants	16	2	8	62%	15%
	Interactions With Health Authority	15	3	5	38%	9%

Vista[1]

Source: Vista1; CEB, now Gartner analysis.
Note: Totals may not equal 100% due to rounding.

a Inherent risk = Likelihood x impact; both on a scale of one to five.
b Residual risk = (likelihood × impact)control effectiveness.
1 Pseudonym.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner

Principle 4

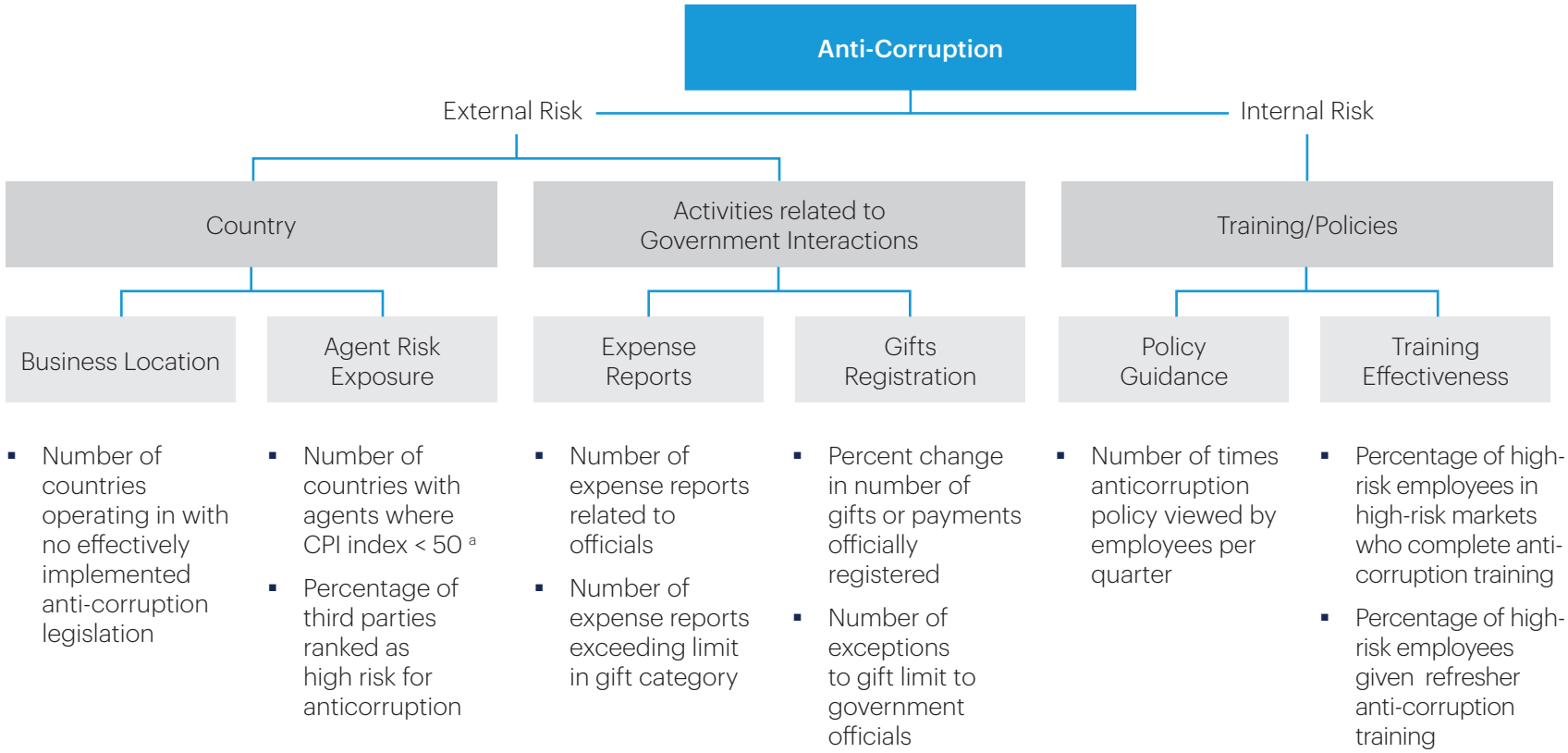
Monitor Risk Drivers

Risk monitoring should efficiently track changes in a company's risk exposure and provide actionable insight into appropriate mitigation.

At its best, monitoring provides realtime information that helps prevent risk events and noncompliance before they occur.

Identification of Risk Drivers

Anti-Corruption Risk Root Causes, Illustrative[a] and Partial



a See Appendix for complete list of KRIs for anti-corruption risk.
Source: CEB, now Gartner Client Company; CEB, now Gartner analysis.
a Transparency International Corruption Perceptions Index.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner

Principle 5

Contextualize Business Decisions

Risk oversight is getting more complicated. Corporate scandals ranging from data breaches to sexual harassment cases have subjected public companies to greater scrutiny while rapidly changing business models mean shifting risk exposures. As a result, legal and compliance must go beyond just reporting information and risk insight into a consumable and business-friendly presentation.

Quarterly Cybersecurity Report

Sample Board Presentation

1Q 2018 Cybersecurity Events

Event Category	Description	Impact (H, M or L)	Mitigation
Lost or Stolen Device	Devices lost or stolen as reported by employees (3)	L	▪ Any mobile device allowed to connect to [company's system] must have company-issued software providing for remote wipe capabilities. ▪ All company-issued laptops have [brand] encryption installed.
Virus Detection on a Server	One file was detected with an embedded malicious code.	L	▪ Updates to anti-virus software were made. ▪ Scans of systems continue to run regularly.

Statistics and Observations

250

Number of phishing attacks blocked weekly

75%

Percentage of targeted employees trained on CAN-SPAM compliance

Insights and Priorities

Reach 100% of targeted employees on CAN-SPAM compliance.

Work with outside counsel to gain understanding of cybersecurity risks presented by business experimentation with new IOT products.

Source: CEB 2016 Board and Governance Survey.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner®

Principle 6

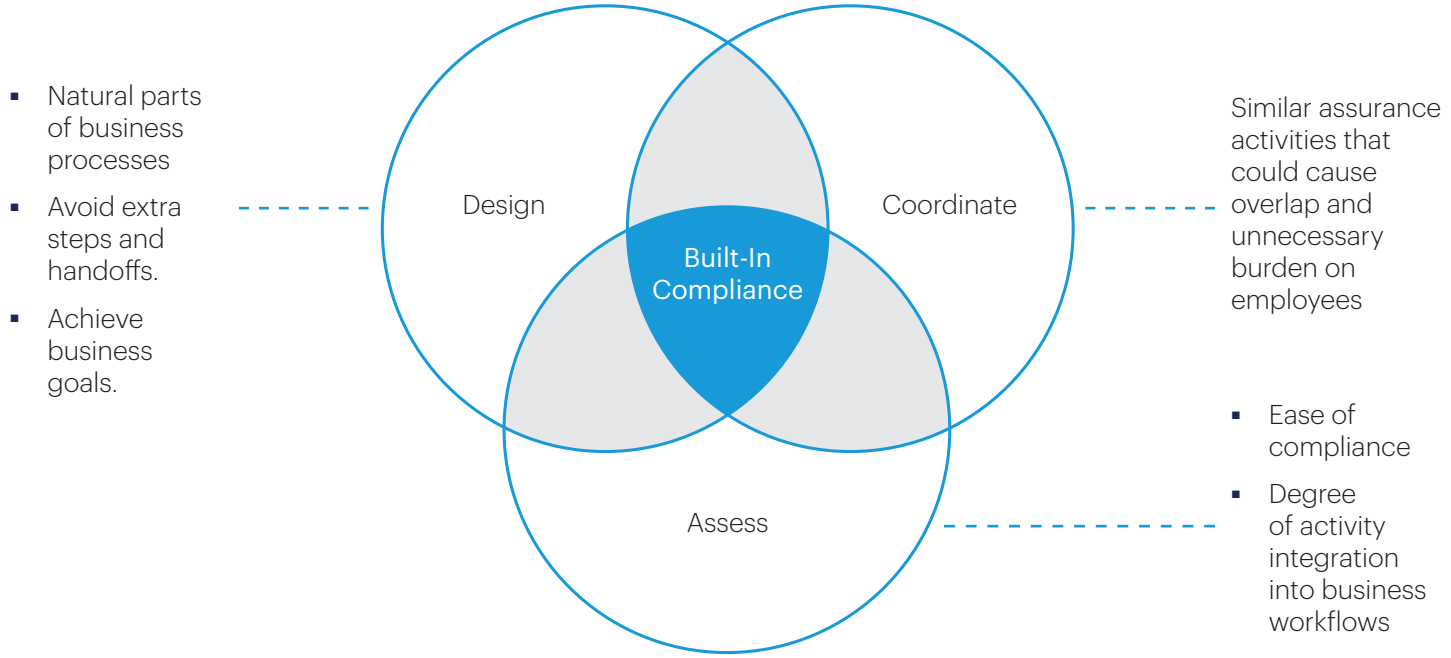
Embed Risk Discipline in Operations

In many cases, legal and compliance risk management activities are separate from business operations, functioning as bolt-ons to common business workflows. The result is both high perceived and real burden of risk advice.

With the increased importance of corporate speed and agility, legal and compliance must coordinate with other assurance functions and embed requirements and guidance into existing processes to provide business leaders with real-time access to risk information.

Components of Built-In Risk Management

Built-in legal and compliance activities are connected to existing workflows or systems, coordinated with related assurance asks of the business and designed to be low-burden on the business.



Source: CEB, now Gartner analysis.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner®

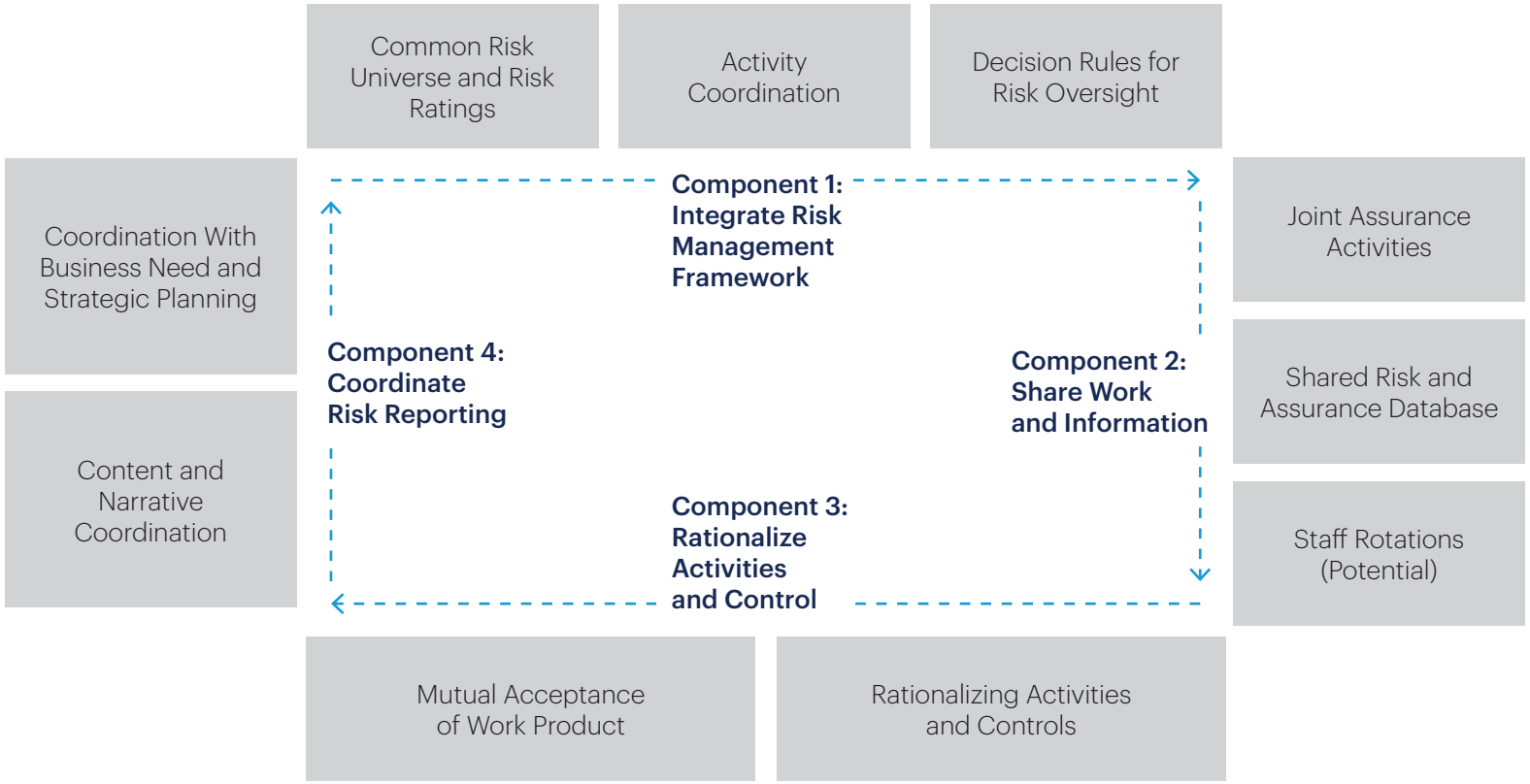
Principle 7

Align Assurance Efforts

At the average company, the number of distinct assurance functions (e.g., compliance, risk, privacy) has doubled over the past decade. Poor alignment of efforts increases the direct cost of assurance, increases operational burden and serves as an anchor on corporate growth.

Going forward, general counsels and compliance executives will be tasked with aligning corporate assurance efforts to provide a holistic view of risk, reduce the total cost of risk management and support achievement of long-term corporate objectives.

Aligned Assurance Framework



Source: Institute of Internal Auditors; CEB, now Gartner analysis.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner®

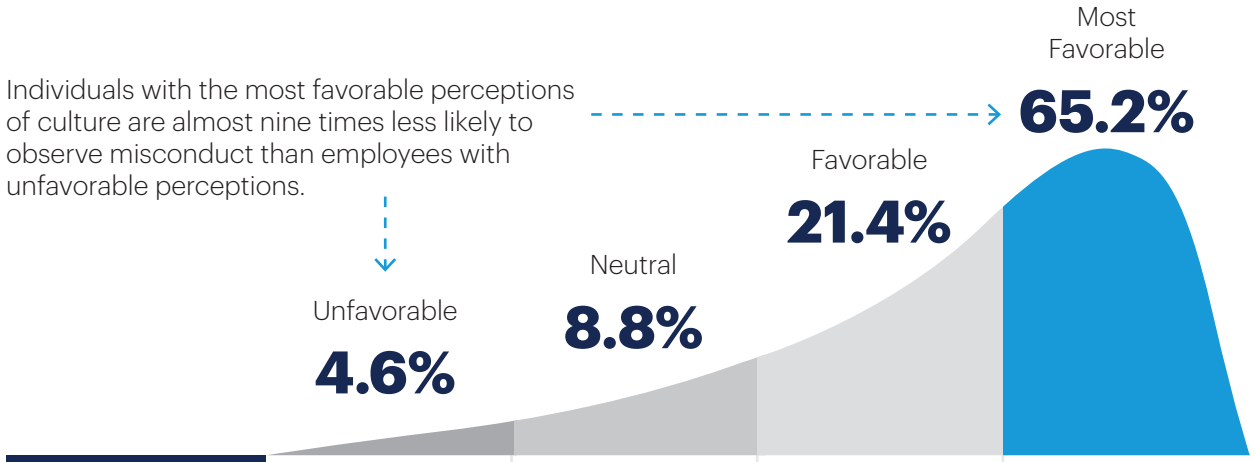
Principle 8

Create a Culture of Integrity

A strong culture of integrity reduces noncompliance and improves reporting. Employees with unfavorable perceptions of company culture observe nearly nine times more misconduct and report 36% less misconduct than employees with the most favorable perceptions of culture. A strong culture means less risk occurs and when it does, executives hear about it more quickly.

The Impact of Culture on Observed and Reported Misconduct

Percentage of Respondents, 2009 to 2016



	Unfavorable	Neutral	Favorable	Most Favorable
Observation Rate[a]	58.4	33.1	16.1	6.5
Reporting Rate[b]	48.4	48.3	54.5	72.9

n = 1,821,514 employees; 233 companies.

The main gains in reporting rate do not emerge until employee perceptions are "most favorable."

Source: CEB 2009-2016 RiskClarity: A Corporate Integrity Service™ Benchmark.
a Percentage of employees within category who observed misconduct in past year.
b Percentage of employees within category who reported the misconduct they observed.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner®

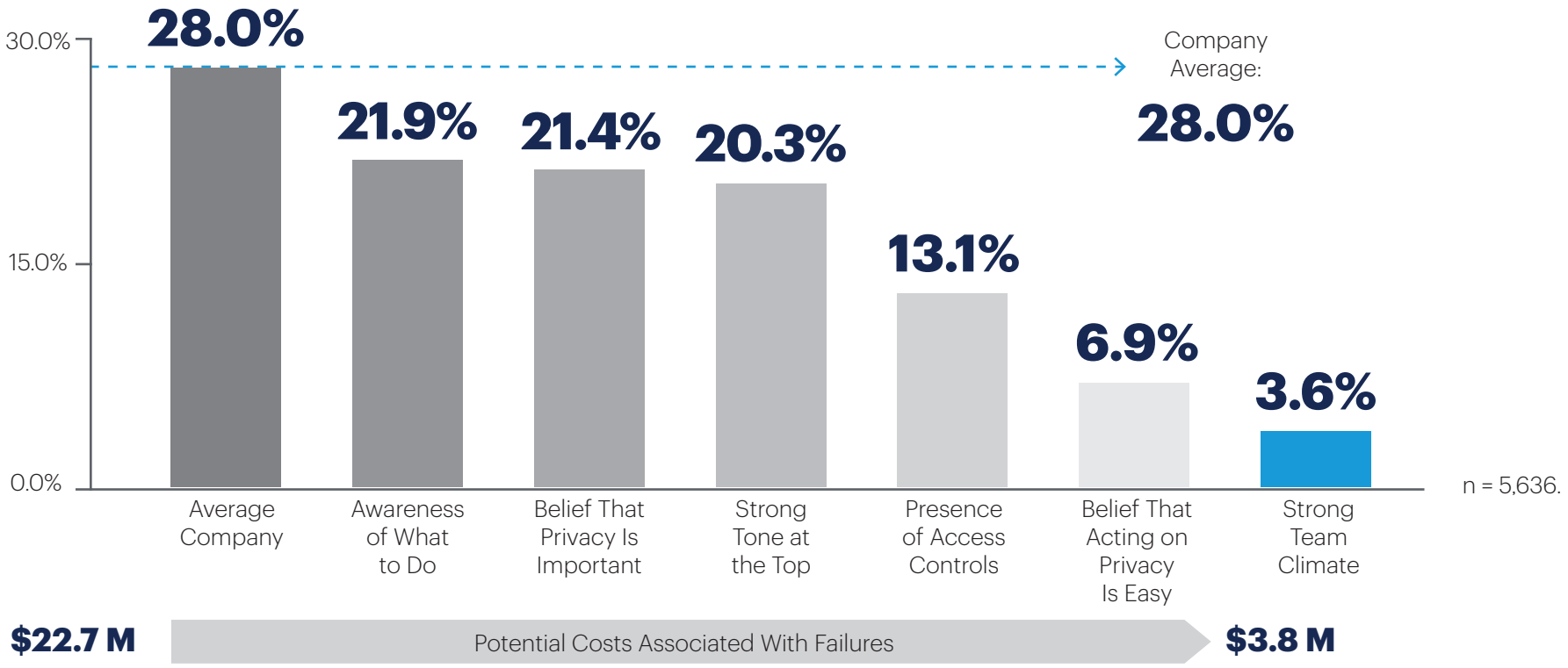
Principle 9

Support Local Climate

The biggest determinant of employees' compliance behavior is how their team behaves. A strong team climate — the group's shared perceptions of the nature of work, including the signals they receive and the processes and practices they follow — has five times the impact of awareness and three times the impact of controls when it comes to improving employees' privacy behaviors. The same result has been found across a range of compliance issues.

Percentage of Employees Exhibiting Poor Privacy Behavior

By Strength of Variable Tested[a]



Source: CEB 2016 Employee Privacy Behavior Assessment.
a Includes employees who on average agreed or strongly agreed with the statements included in each variable.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner

Principle 10

Improve Information Flows

While data is more abundant than ever, general counsels (GCs) and chief compliance officers (CCOs) struggle to collect known information about legal and compliance risks.

Only 13% of known information about potential misconduct actually makes it to the compliance function, limiting the ability to understand behavior and mitigate risks.

Misconduct Information Reporting Lines

Council Schematic of Information Flows

Information Lost

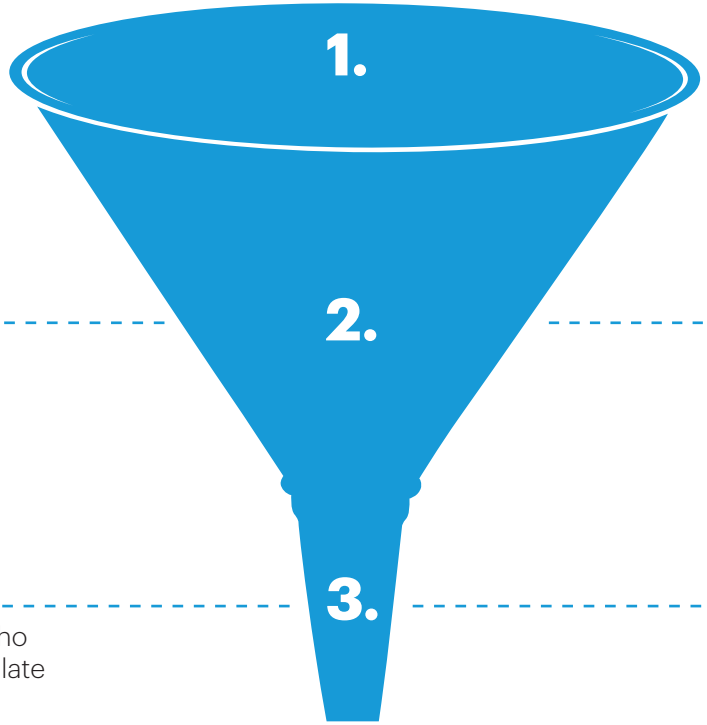
More than half percent of observed business misconduct is never reported by employees.

Information Stuck

More than two-thirds of reported misconduct information is directly reported to managers.

Information Siloed

Nearly three-quarters of managers who receive misconduct information escalate that information to their manager.



Only a small amount of potential misconduct information makes it to the compliance function.

Observed Misconduct Information[a]

Steps to Improve Employee Reporting

1. Establish and promote reporting channels.
2. Create a company wide speaking-up policy.
3. Issue communications that address employee fears of retaliation.

Steps to Train Managers to Respond to Misconduct

1. Train managers on how to respond appropriately to employee reports of misconduct.
2. Provide managers with tools and resources to discuss the investigation process with employees.

Steps to Ensure Consistent Response to Misconduct

1. Create clear escalation criteria for managers and senior executives.
2. Raise awareness about the escalation criteria.

Source: CEB, now Gartner analysis.
a For example, harassment, insider trading, fraud.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner®

Contact Us to Learn More

Phone:
+1-866-913-8103

E-mail:
LegalComplianceLeaders@gartner.com

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.
For more information, email info@gartner.com or visit gartner.com.

Gartner®