Tuesday, October 2, 2012
11:00 AM - 12:30 PM

1205 – Risk Assessment Best Practices: Lessons from Compliance Programs

Christine Connolly
Vice President, Corporate Secretary & Chief Compliance Officer
Dollar General Corporation

Christopher Goddard
Associate General Counsel
Washington University in St. Louis

Patricia Hanz
Assistant General Counsel
Briggs & Stratton Corporation

Amy Hutchens
General Counsel, Vice President
Watermark Risk Management International, LLC

Faculty Biographies

Christine Connolly

Christine Connolly is vice president, corporate secretary and chief compliance officer of Dollar General Corporation, the largest discount retailer in the United States by number of stores.

In addition to overseeing board and governance-related matters, she advises the company on Securities Exchange Act and Securities Act matters and New York Stock Exchange compliance. She also coordinates Dollar General's umbrella compliance program, including chairing the executive compliance committee and overseeing the risk assessment process. Prior to Dollar General, Ms. Connolly practiced law as an associate with Dinsmore & Shohl LLP and Thompson Coburn LLP, focusing on securities law, mergers and acquisitions and general corporate law.

Ms. Connolly earned a BS from Missouri State University and JD from Vanderbilt University School of Law.

Christopher Goddard

Christopher W. Goddard is associate general counsel for Washington University in St. Louis. His responsibilities cover a wide spectrum of corporate, litigation, and healthcare activities. He devotes a substantial portion of his practice to regulatory and corporate compliance in areas such as federal grants and contracts, physician billing, data privacy and security, international initiatives, export controls, and environmental health and safety. He also handles software licensing, litigation management, and insurance matters.

Prior to joining Washington University, Mr. Goddard served as a special assistant United States attorney for the eastern district of Missouri and as a law clerk to the Honorable Raymond W. Gruender, U.S. Court of Appeals for the Eighth Circuit. He is also an adjunct professor for Washington University School of Law.

Mr. Goddard serves on the board of directors for the ACC's St. Louis Chapter. He is a member of the National Association of College and University Attorneys. His civic involvement has included various roles with the Juvenile Diabetes Research Foundation, the Donald Danforth Plant Science Center, and the Ronald McDonald House Charities.

Mr. Goddard received his BA from the University of Notre Dame and his JD from Washington University School of Law.

Patricia Hanz

Assistant General Counsel
Briggs & Stratton Corporation

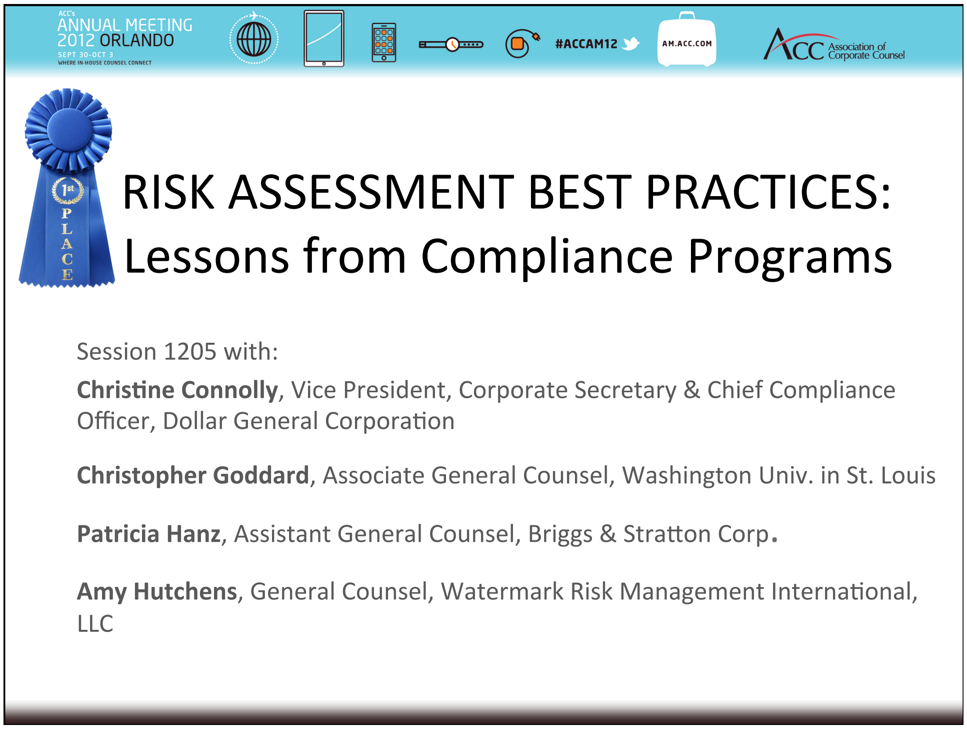
Amy Hutchens

Amy Hutchens is certified by the Society of Corporate Compliance and Ethics as a Corporate Compliance and Ethics Professional (CCEP) and currently serves as Watermark's general counsel and vice president of compliance and ethics services. She works with corporations assisting with development of the compliance and ethics infrastructure required by the Federal Sentencing Guidelines and Federal Acquisition Regulation. She has developed, implemented, and managed all aspects of compliance programs including assessing risk, drafting policies, training employees, developing codes of conduct, and establishing monitoring and investigative protocols to maximize value and effectiveness in compliance and ethics programs.

Previously, Ms. Hutchens was a special assistant United States attorney and an Air Force Judge Advocate, attaining the rank of Major, before beginning her civilian career in-house. She has federal litigation experience, as well as experience advising executive management on personnel, compliance and ethics matters.

As a veteran herself and the spouse of a 100% combat disabled veteran, Ms. Hutchens dedicates her pro bono time to assisting military veterans with a range of legal issues. She is a volunteer attorney with the Virginia State Bar Veteran's Initiative and is active in her retired/reserve Judge Advocate General's network.

Ms. Hutchens is a graduate of the Johns Hopkins Peabody Conservatory of Music, and Vanderbilt University School of Law.



ACC's ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT
#ACCAM12
AM.ACC.COM
ACC Association of Corporate Counsel
1st PLACE

RISK ASSESSMENT BEST PRACTICES: Lessons from Compliance Programs

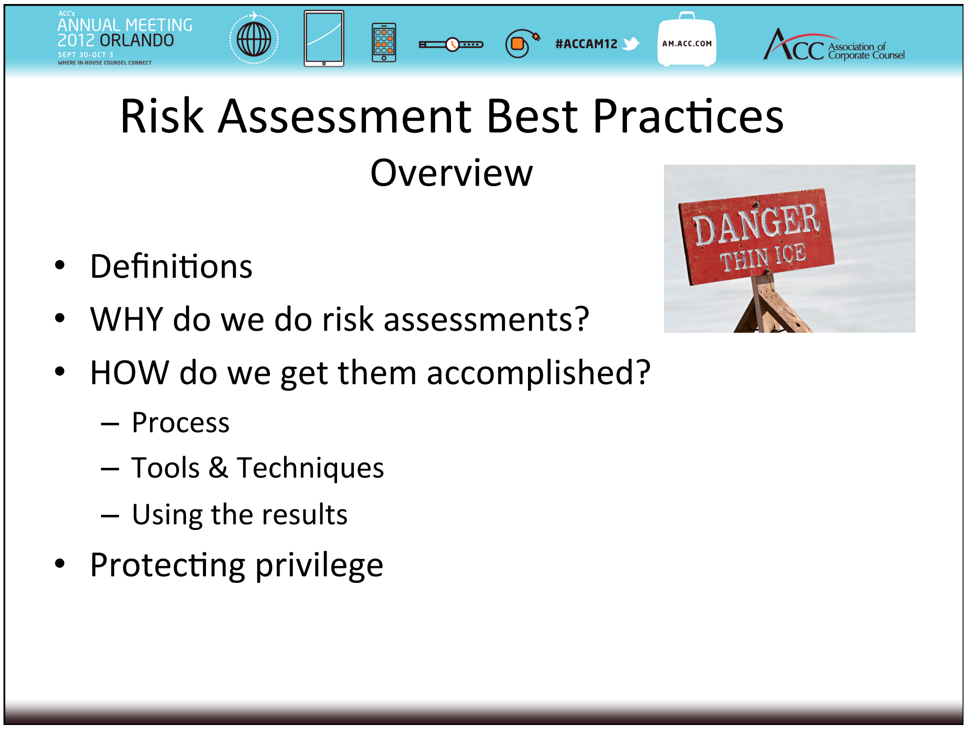
Session 1205 with:

Christine Connolly, Vice President, Corporate Secretary & Chief Compliance Officer, Dollar General Corporation

Christopher Goddard, Associate General Counsel, Washington Univ. in St. Louis

Patricia Hanz, Assistant General Counsel, Briggs & Stratton Corp.

Amy Hutchens, General Counsel, Watermark Risk Management International, LLC

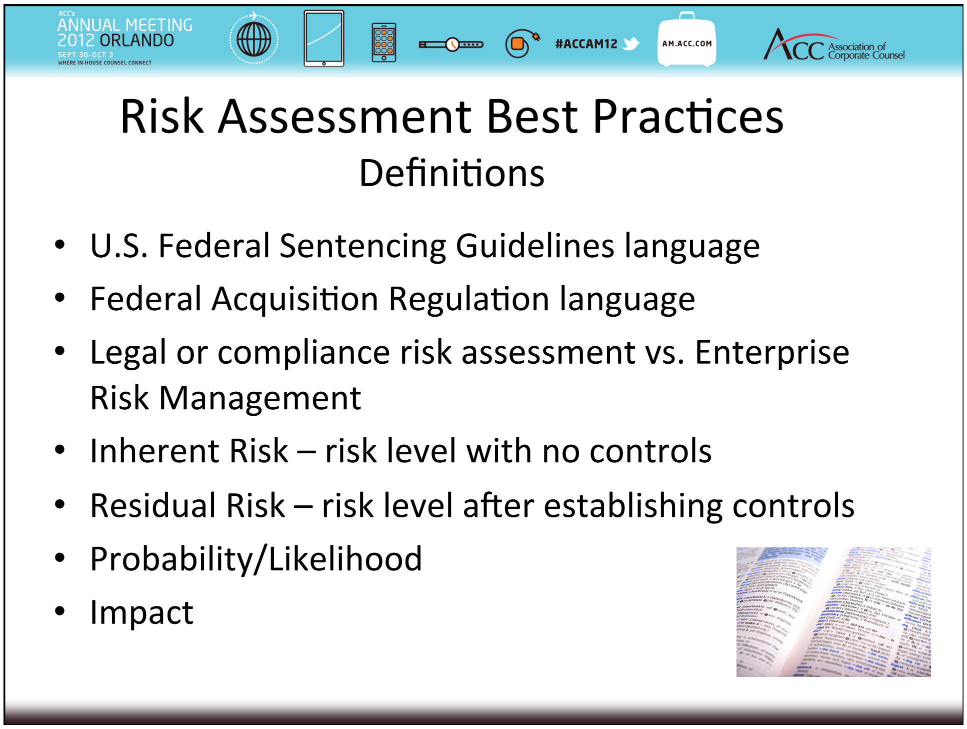


ACC's ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT
#ACCAM12
AM.ACC.COM
ACC Association of Corporate Counsel
DANGER
THIN ICE

Risk Assessment Best Practices

Overview

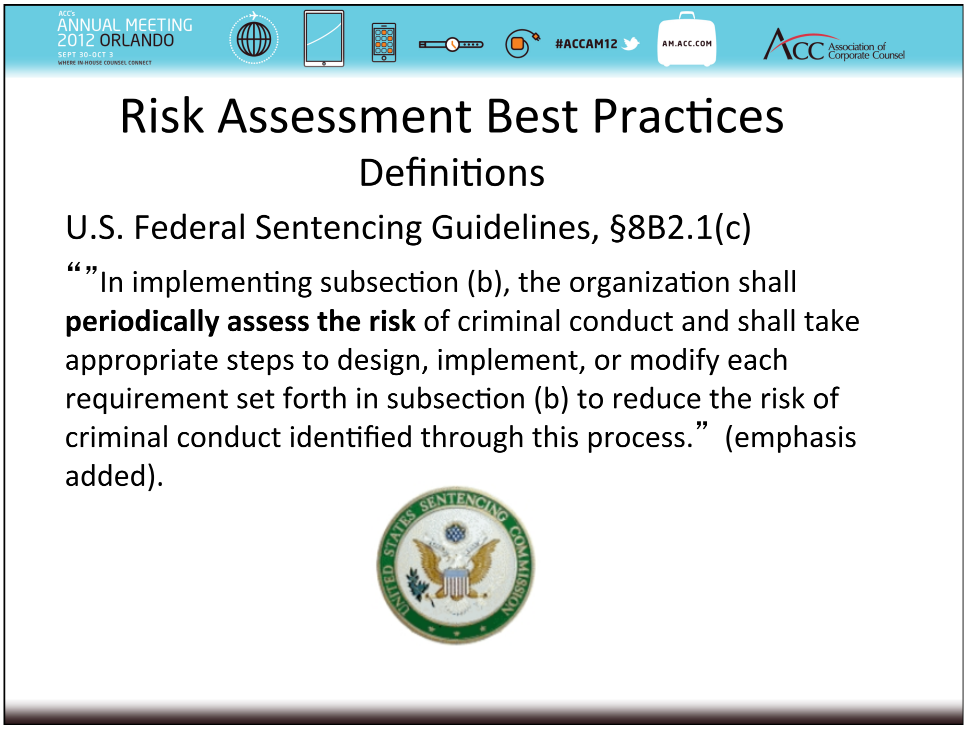
- Definitions
- WHY do we do risk assessments?
- HOW do we get them accomplished?
  - Process
  - Tools & Techniques
  - Using the results
- Protecting privilege



Risk Assessment Best Practices

Definitions

- U.S. Federal Sentencing Guidelines language
- Federal Acquisition Regulation language
- Legal or compliance risk assessment vs. Enterprise Risk Management
- Inherent Risk – risk level with no controls
- Residual Risk – risk level after establishing controls
- Probability/Likelihood
- Impact

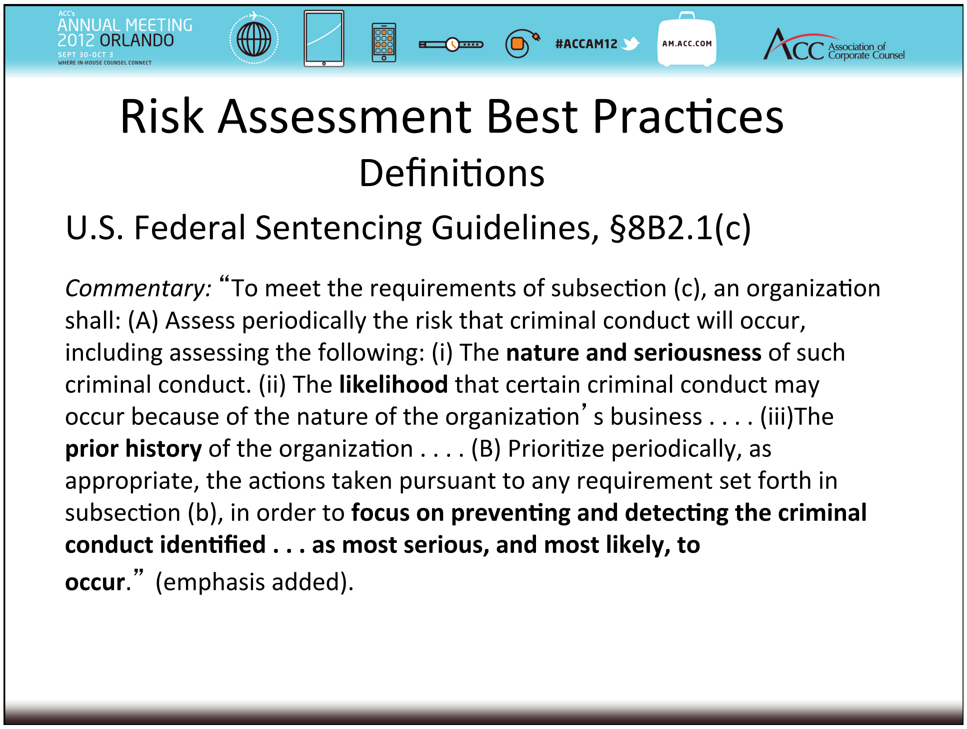


Risk Assessment Best Practices

Definitions

U.S. Federal Sentencing Guidelines, §8B2.1(c)

“”In implementing subsection (b), the organization shall **periodically assess the risk** of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.” (emphasis added).

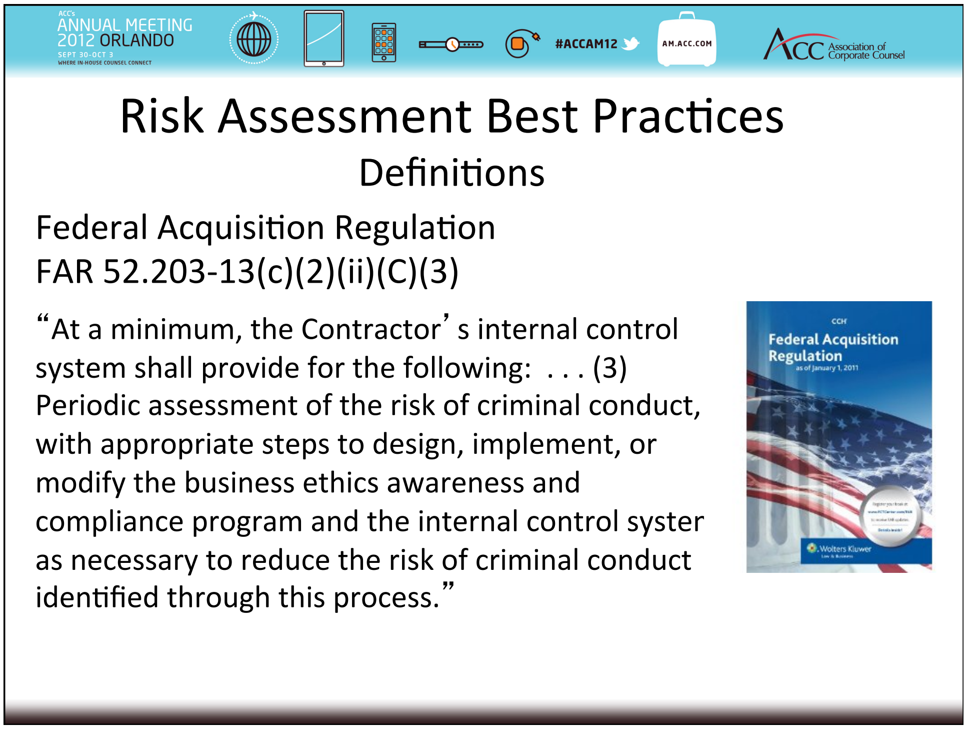

ACC's ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT
#ACCAM12
AM.ACC.COM
ACC Association of Corporate Counsel

Risk Assessment Best Practices

Definitions

U.S. Federal Sentencing Guidelines, §8B2.1(c)

Commentary: “To meet the requirements of subsection (c), an organization shall: (A) Assess periodically the risk that criminal conduct will occur, including assessing the following: (i) The **nature and seriousness** of such criminal conduct. (ii) The **likelihood** that certain criminal conduct may occur because of the nature of the organization’ s business . . . . (iii)The **prior history** of the organization . . . . (B) Prioritize periodically, as appropriate, the actions taken pursuant to any requirement set forth in subsection (b), in order to **focus on preventing and detecting the criminal conduct identified . . . as most serious, and most likely, to occur**.” (emphasis added).

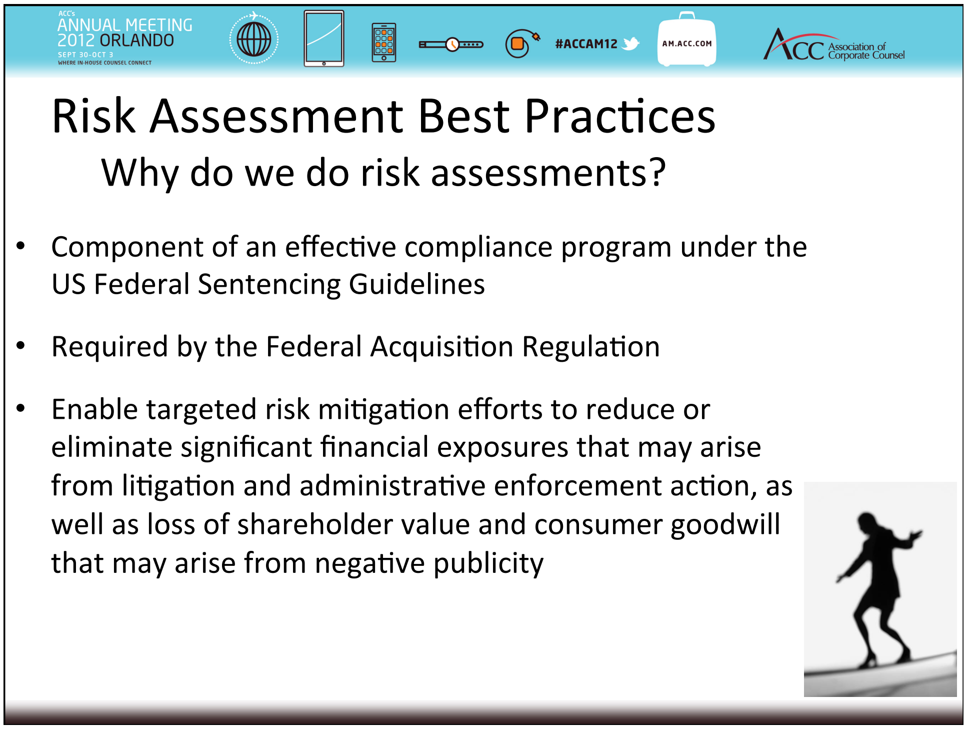

ACC's ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT
#ACCAM12
AM.ACC.COM
ACC Association of Corporate Counsel
CCH
Federal Acquisition Regulation
as of January 1, 2011
Wolters Kluwer Law & Business

Risk Assessment Best Practices

Definitions

Federal Acquisition Regulation FAR 52.203-13(c)(2)(ii)(C)(3)

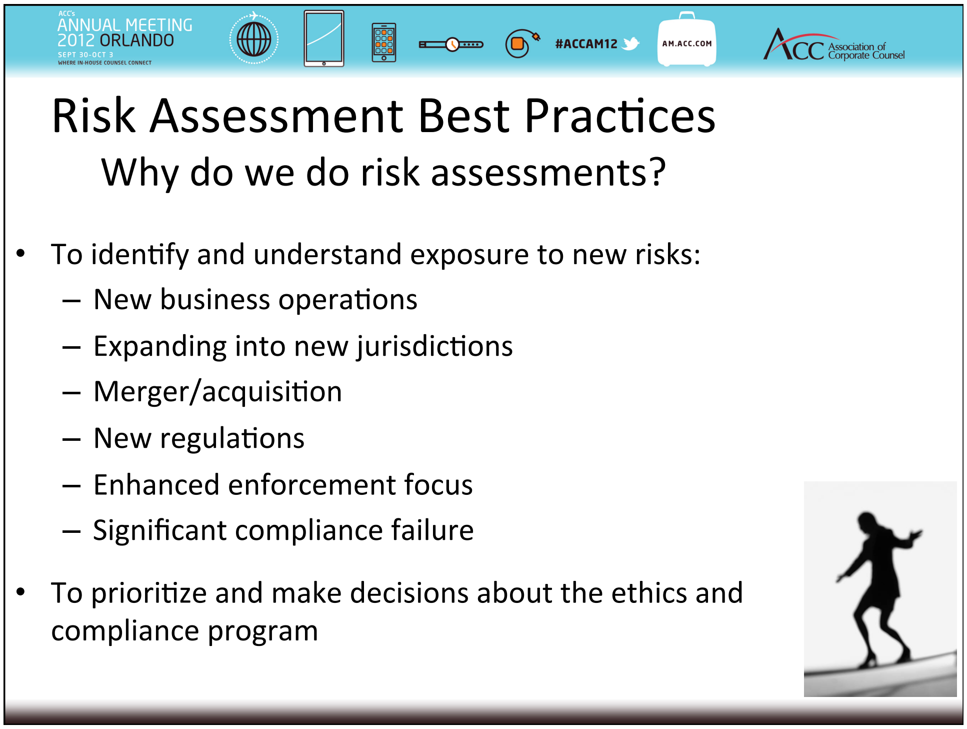
“At a minimum, the Contractor’ s internal control system shall provide for the following: . . . (3) Periodic assessment of the risk of criminal conduct, with appropriate steps to design, implement, or modify the business ethics awareness and compliance program and the internal control syster as necessary to reduce the risk of criminal conduct identified through this process.”



Risk Assessment Best Practices

Why do we do risk assessments?

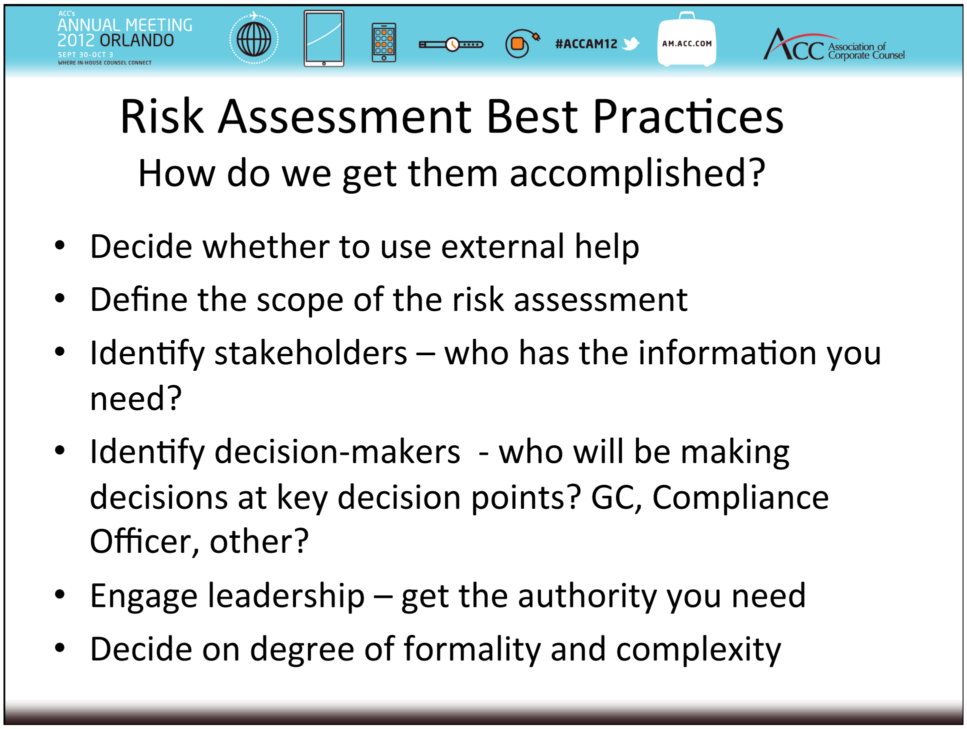
- Component of an effective compliance program under the US Federal Sentencing Guidelines
- Required by the Federal Acquisition Regulation
- Enable targeted risk mitigation efforts to reduce or eliminate significant financial exposures that may arise from litigation and administrative enforcement action, as well as loss of shareholder value and consumer goodwill that may arise from negative publicity



Risk Assessment Best Practices

Why do we do risk assessments?

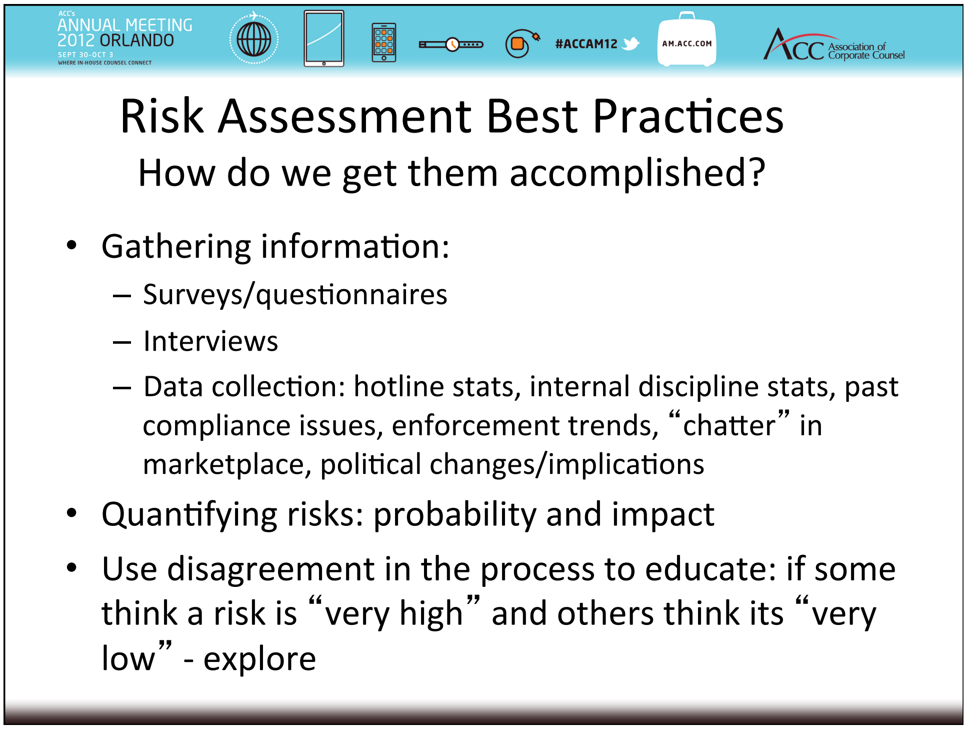
- To identify and understand exposure to new risks:
  - New business operations
  - Expanding into new jurisdictions
  - Merger/acquisition
  - New regulations
  - Enhanced enforcement focus
  - Significant compliance failure
- To prioritize and make decisions about the ethics and compliance program



Risk Assessment Best Practices

How do we get them accomplished?

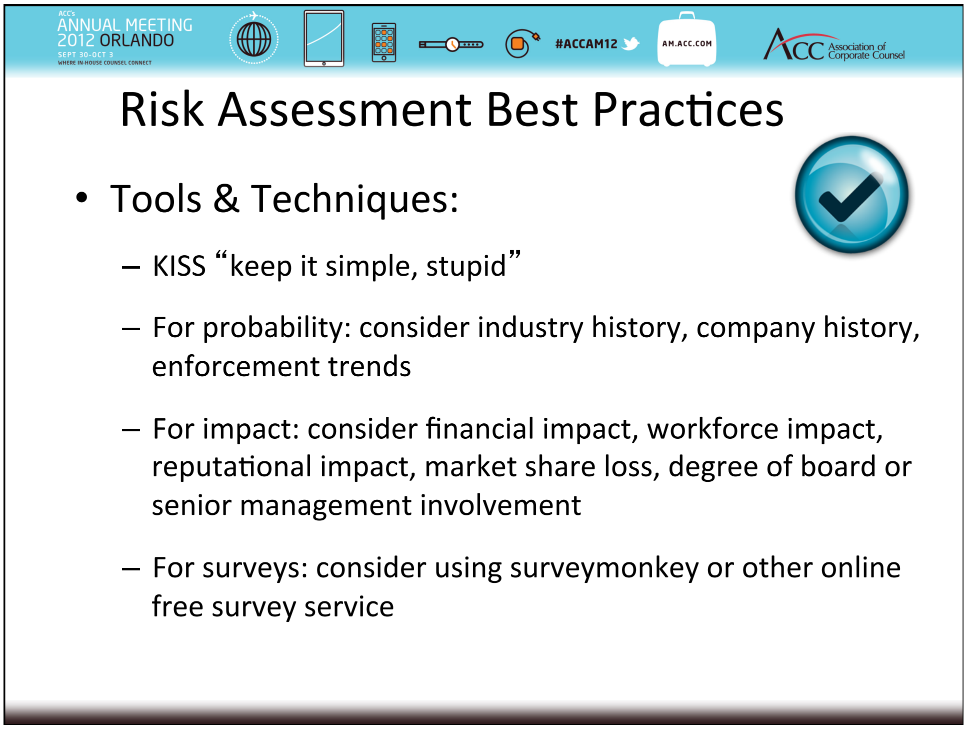
- Decide whether to use external help
- Define the scope of the risk assessment
- Identify stakeholders – who has the information you need?
- Identify decision-makers - who will be making decisions at key decision points? GC, Compliance Officer, other?
- Engage leadership – get the authority you need
- Decide on degree of formality and complexity



Risk Assessment Best Practices

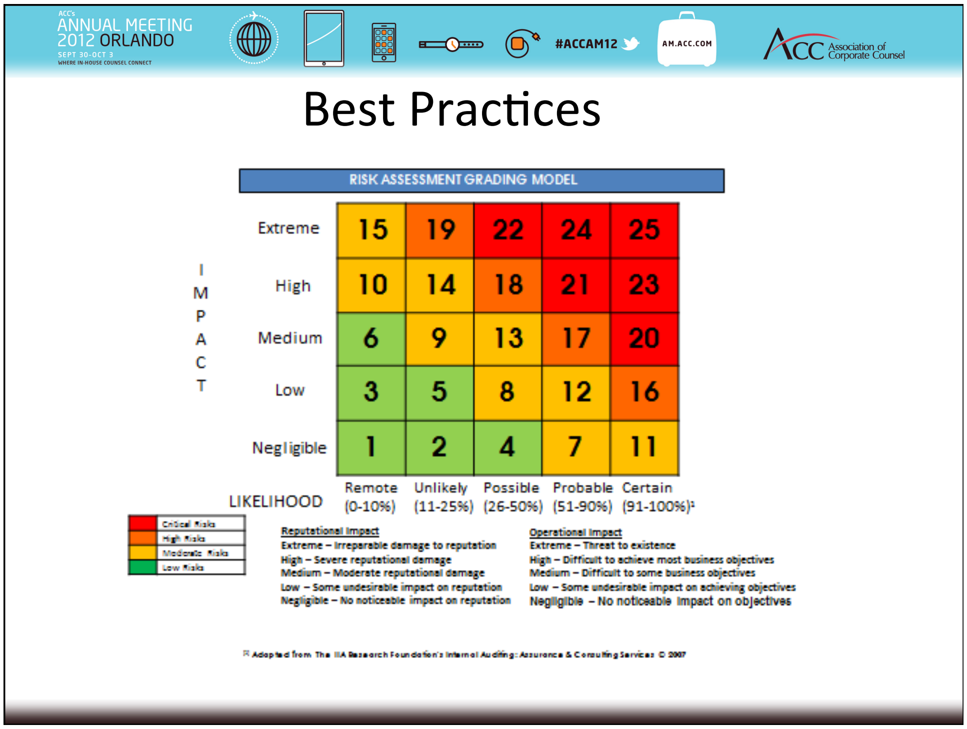
How do we get them accomplished?

- Gathering information:
  - Surveys/questionnaires
  - Interviews
  - Data collection: hotline stats, internal discipline stats, past compliance issues, enforcement trends, “chatter” in marketplace, political changes/implications
- Quantifying risks: probability and impact
- Use disagreement in the process to educate: if some think a risk is “very high” and others think its “very low” - explore


ACC's ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT
#ACCAM12
AM.ACC.COM
ACC Association of Corporate Counsel

Risk Assessment Best Practices

- Tools & Techniques:
  - KISS "keep it simple, stupid"
  - For probability: consider industry history, company history, enforcement trends
  - For impact: consider financial impact, workforce impact, reputational impact, market share loss, degree of board or senior management involvement
  - For surveys: consider using surveymonkey or other online free survey service


ACC's ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT
#ACCAM12
AM.ACC.COM
ACC Association of Corporate Counsel

Best Practices

RISK ASSESSMENT GRADING MODEL

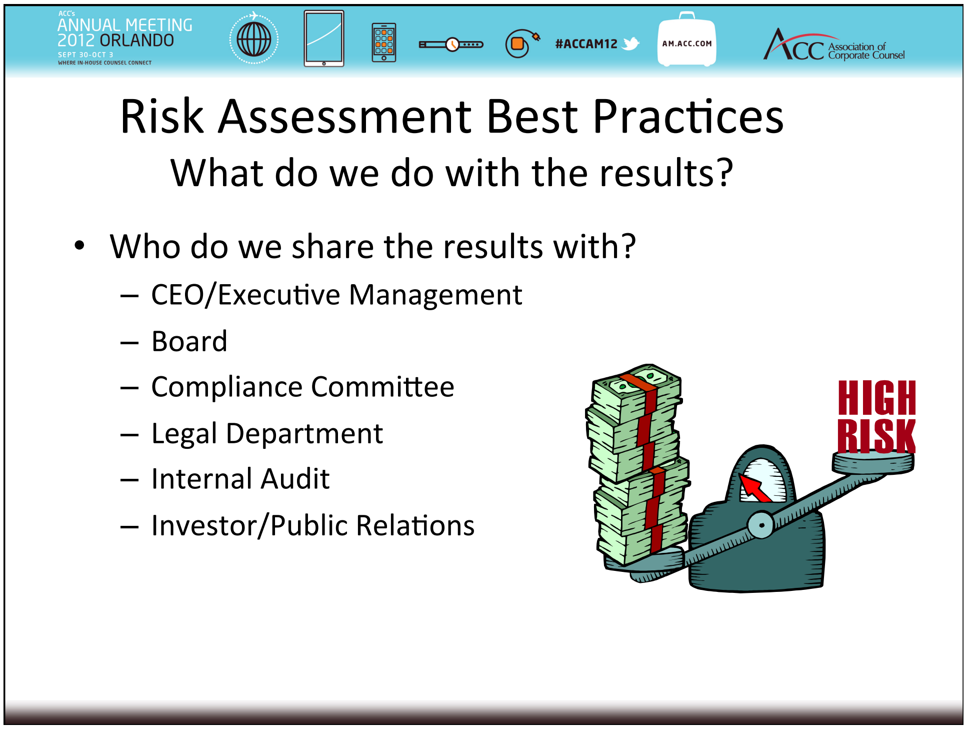
IMPACT					
Extreme	15	19	22	24	25
High	10	14	18	21	23
Medium	6	9	13	17	20
Low	3	5	8	12	16
Negligible	1	2	4	7	11
LIKELIHOOD	Remote (0-10%)	Unlikely (11-25%)	Possible (26-50%)	Probable (51-90%)	Certain (91-100%)[1]

🟥	Critical Risks
🟧	High Risks
🟨	Moderate Risks
🟩	Low Risks

Reputational Impact
Extreme – Irreparable damage to reputation
High – Severe reputational damage
Medium – Moderate reputational damage
Low – Some undesirable impact on reputation
Negligible – No noticeable impact on reputation

Operational Impact
Extreme – Threat to existence
High – Difficult to achieve most business objectives
Medium – Difficult to some business objectives
Low – Some undesirable impact on achieving objectives
Negligible – No noticeable impact on objectives

[1] Adapted from The IIA Research Foundation's Internal Auditing: Assurance & Consulting Services © 2007

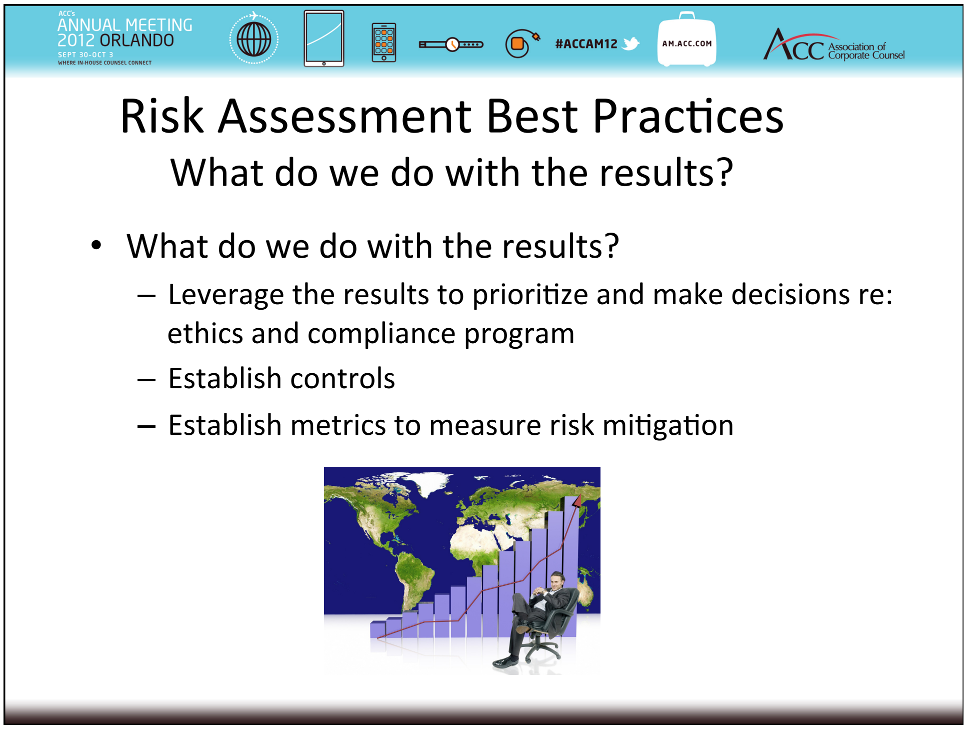


ACC's ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT
#ACCAM12
AM.ACC.COM
ACC Association of Corporate Counsel
HIGH RISK

Risk Assessment Best Practices

What do we do with the results?

- Who do we share the results with?
  - CEO/Executive Management
  - Board
  - Compliance Committee
  - Legal Department
  - Internal Audit
  - Investor/Public Relations

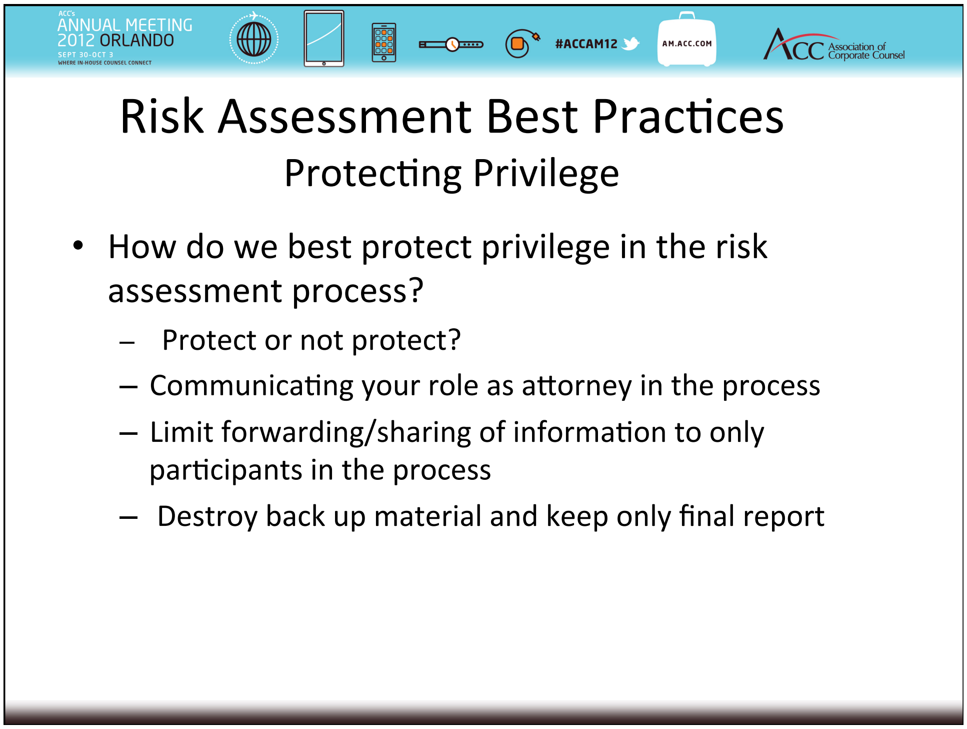


ACC's ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT
#ACCAM12
AM.ACC.COM
ACC Association of Corporate Counsel

Risk Assessment Best Practices

What do we do with the results?

- What do we do with the results?
  - Leverage the results to prioritize and make decisions re: ethics and compliance program
  - Establish controls
  - Establish metrics to measure risk mitigation


ACC's ANNUAL MEETING 2012 ORLANDO
SEPT 30-OCT 3
WHERE IN-HOUSE COUNSEL CONNECT
#ACCAM12
AM.ACC.COM
ACC Association of Corporate Counsel

Risk Assessment Best Practices

Protecting Privilege

- How do we best protect privilege in the risk assessment process?
  - Protect or not protect?
  - Communicating your role as attorney in the process
  - Limit forwarding/sharing of information to only participants in the process
  - Destroy back up material and keep only final report

RISK ASSESSMENT GRADING MODEL

IMPACT LIKELIHOOD	Remote (0-10%)	Unlikely (11-25%)	Possible (26-50%)	Probable (51-90%)	Certain (91-100%)[1]
Extreme	🟨 15	🟧 19	🟥 22	🟥 24	🟥 25
High	🟨 10	🟨 14	🟧 18	🟥 21	🟥 23
Medium	🟩 6	🟨 9	🟨 13	🟧 17	🟥 20
Low	🟩 3	🟩 5	🟨 8	🟨 12	🟧 16
Negligible	🟩 1	🟩 2	🟩 4	🟨 7	🟨 11

🟥	Critical Risks
🟧	High Risks
🟨	Moderate Risks
🟩	Low Risks

Reputational Impact

Extreme – Irreparable damage to reputation
High – Severe reputational damage
Medium – Moderate reputational damage
Low – Some undesirable impact on reputation
Negligible – No noticeable impact on reputation

Operational Impact

Extreme – Threat to existence
High – Difficult to achieve most business objectives
Medium – Difficult to some business objectives
Low – Some undesirable impact on achieving objectives
Negligible – No noticeable impact on objectives

[1] Adapted from The IIA Research Foundation's Internal Auditing: Assurance & Consulting Services © 2007

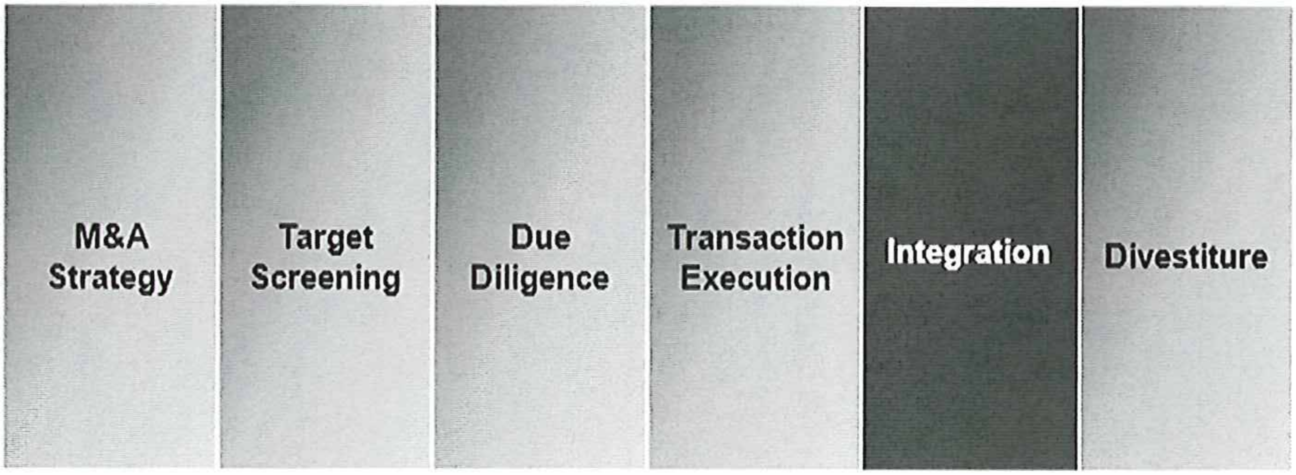
Legal Risk Assessments
Key Decision Points and Relevant Considerations

Key Decision Point	Relevant Considerations
Who directs the risk assessment--outside advisor or in-house personnel?	• Degree of regulation/complexity of the industry and business • Degree of complexity of the assessment • Experience level of in-house personnel • Time/resource constraints
Who participates	• Compliance committee members/compliance department personnel • Anyone else? o Executive management o Full officer group o Senior manager level o Legal o Internal Audit o Other • Participate in entire process or just parts (e.g., identification, evaluation, next steps)
What is the scope	• Legal and ethical risks or just legal risks? • All legal risks or just those with criminal penalties? • Include local regulations? • Include risks in addition to legal/ethical, such as enterprise risk management? • Specific or multiple risk areas?
Degree of formality and complexity of procedure	• Degree of regulation/complexity of the industry and business • Experience level of personnel directing the assessment • Time/resource constraints • Purpose/goals of the assessment
Measuring Probability and Impact: Quantitative, Qualitative or Some Combination	• Need for consistent reference points for participants (tend towards use of quantitative measures) • Need for "reigning in" participants who tend to rank "all or nothing" (tend towards use of quantitative measures)

	• Style of risk assessment (i.e., primarily interview-based and final rankings determined by person directing the assessment, tend towards use of qualitative measures; primarily questionnaire-based and final rankings determined by weighted average, tend towards use of quantitative measures) • Expectations of those who will receive and use the report
What is the Purpose	• Federal Sentencing Guidelines • Resource allocation • Standalone legal risk v. piece of enterprise risk management • Proactive v. reactive
Reporting	• Who needs the report (Board, compliance committee/compliance department, executive management, legal, internal audit, others?) • Are you trying to protect the privilege
Action Plan for Results	• Depends on the purpose for the assessment • Time/resource limitations • Remember the need for flexibility (i.e., ability to modify the action plan as circumstances change) • Who will follow up on the action plan • Who will report on the status of the action plan, and to whom • What happens if a responsible party drops the ball on the action plan
How often to conduct the assessment	• What is the purpose of the assessment • What are the expectations of the person(s) requesting the assessment • Degree of regulation/complexity of the business and its industry • Frequency with which the business changes • Frequency with which the laws/regulations that govern the business change • Has an intervening event occurred (e.g., merger/acquisition, major compliance failure by a company in the industry or by the company itself, etc.)
Who decides all the above (e.g., GC or CCO either with or without oversight of a compliance committee, the Board or a Board committee)	• Company culture • Degree of formality of the assessment process • Trying to maintain privilege?

INTEGRATION GUIDE

BRIGGS & STRATTON CORPORATION



M&A Strategy

Target Screening

Due Diligence

Transaction Execution

Integration

Divestiture

CONTENTS

1. INTEGRATION OVERVIEW

1.1 Executive Summary

The objective of the Integration Guide is to provide a framework, process, and tools for integrating an acquired company. The framework outlined in the guide serves as a baseline for integrating every acquisition. However, the process and tools described within the guide may be tailored to fit the strategic objectives of each unique acquisition.

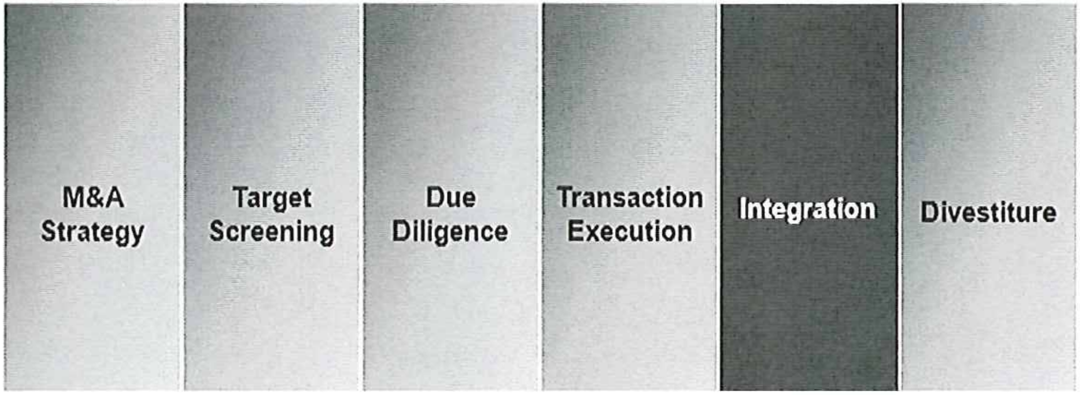
The guide will be continually updated by Corporate Development with input from integration team members to incorporate best practices and process improvements.

1.2 Integration Defined

Integration is unlocking the acquisition value by executing a scalable plan to comply with, combine or enhance business processes.

This guide outlines integration as a single phase in the Merger and Acquisition (M&A) lifecycle; however, the success of integration depends on appropriate planning and execution of key activities during earlier phases in the lifecycle (i.e. due diligence, transaction execution).

M&A Lifecycle:



M&A Strategy

Target Screening

Due Diligence

Transaction Execution

Integration

Divestiture

1.3 Guiding Principles

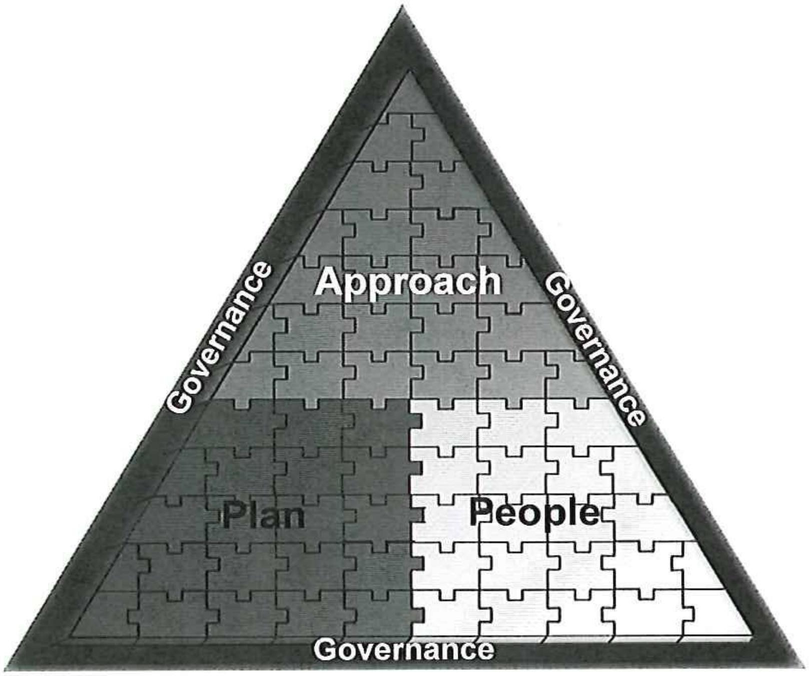
The *Integration Guide* is based on four principles to help maintain focus on acquisition value drivers and improve integration results. Those Guiding Principles are as follows:

Approach
The business strategy drives the integration approach which drives the integration plan.

Plan
The integration plan should be created in the due diligence phase, be time based and consist of negotiables, non-negotiables and default positions.

People
A dedicated integration leader is accountable for the integration plan and execution. Functional integration teams execute the integration plan.

Governance
A governance model provides strategic guidance and oversees integration performance and issue resolution.



1.4 Keys to Integration Success

Benefits of this integration process can be linked to the Guiding Principles as follows:

Approach

- Aligns the integration plan to the business strategy
- Encourages alignment of senior leadership and key stakeholders regarding strategy, integration priorities, resource utilization and timing
- Facilitates communication of scope and prioritization of initiatives most critical to integration success
- Administers a consistent but scalable process regardless of acquisition size or type

Plan

- Focuses teams and detailed plans on most critical initiatives
- Standardized tools and templates to foster rapid implementation and capture results
- Emphasizes the first 90-days to make changes
- Identifies non-negotiable and default positions to facilitate timely and thorough planning

People

- Creates focus and accountability by assigning a full-time integration leader
- Separates the integration efforts from the ongoing business efforts
- Defines roles and responsibilities for all integration team members
- Identifies individuals responsible for key decisions
- Communication practices are consistent and relevant throughout the organization

Governance

- Ensures Approach, Plan, and People principles stay aligned to business strategy
- Provides scope and decision guidance to ensure integration efforts stay on course
- Consistent framework for individual responsible and accountable for integration
- Establishes a standard process for monitoring and measuring success

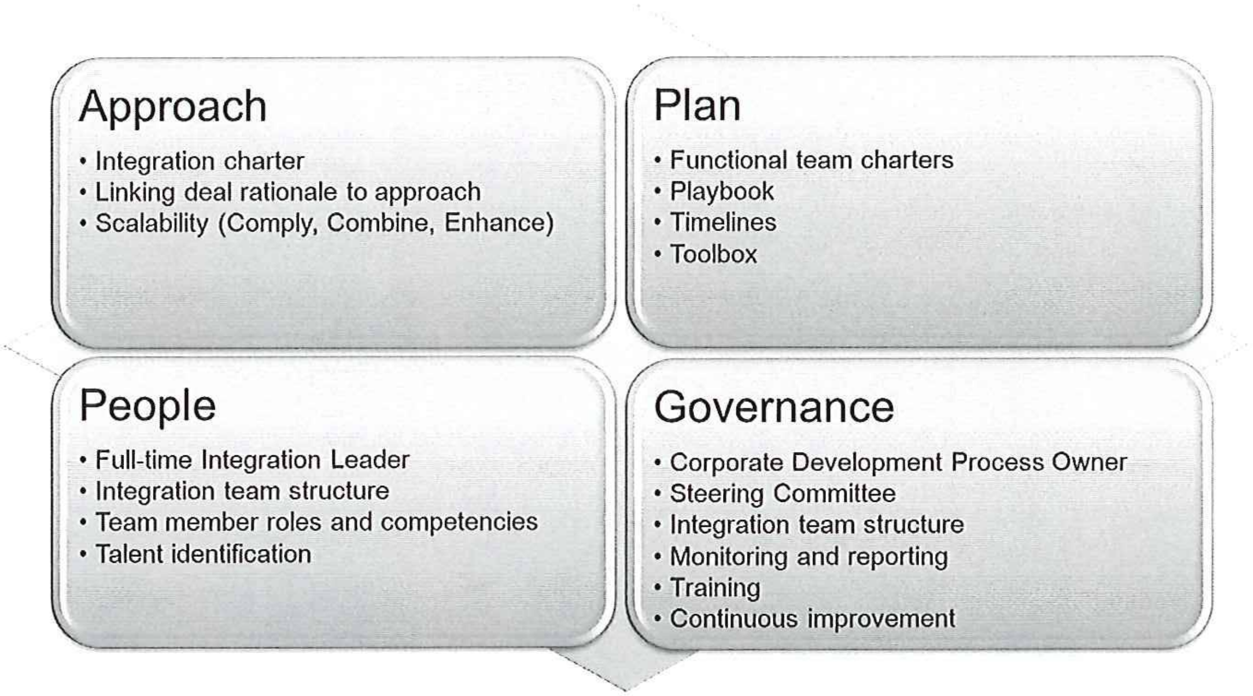
1.5 Common Integration Pitfalls

Common integration pitfalls and the corresponding link to the Guiding Principles are as follows:

Category	Pitfall
Approach	• Focus on standardizing organizations rather than capturing value • Losing sight of the customer or other key stakeholders critical to the business • Stopping short of significant change (Reinforcing status quo) • Lack of focus and clear articulation results in business disruption and wasted effort • Underestimating the challenges • Slow and passive actions instead of quick and decisive
Plan	• Not developing integration plan prior to day 1 • Not leveraging the findings from due diligence into the integration plan • Integration activities happen too slowly, fail to capitalize on expectation of change • Vague or delayed communications • Assuming all employees have the same level of understanding of the acquisition and / or integration • Widespread confusion about the company identity, mission, and goals
People	• Combining the integration leader and business leader into a single role reduces focus on integration • Lack of a clearly defined integration leader • Not having the integration leader involved in due diligence • Lack of clarity on roles and responsibilities including decision making • Underresourcing the integration efforts • People assessment not performed early enough • Assuming a prevailing culture or focusing on culture comparisons between the two organizations
Governance	• Losing sight of the acquisition value and strategic objectives • Losing alignment of business strategy and integration approach • Lack of oversight to drive accountability and resolve issues • Lack of meaningful metrics

1.6 Guiding Principles in Practice

The organization and contents of the Integration Guide advance the four Guiding Principles into practice. Listed below are the practical elements of the Integration Guide and the corresponding Guiding Principle.



Approach

- Integration charter
- Linking deal rationale to approach
- Scalability (Comply, Combine, Enhance)

Plan

- Functional team charters
- Playbook
- Timelines
- Toolbox

People

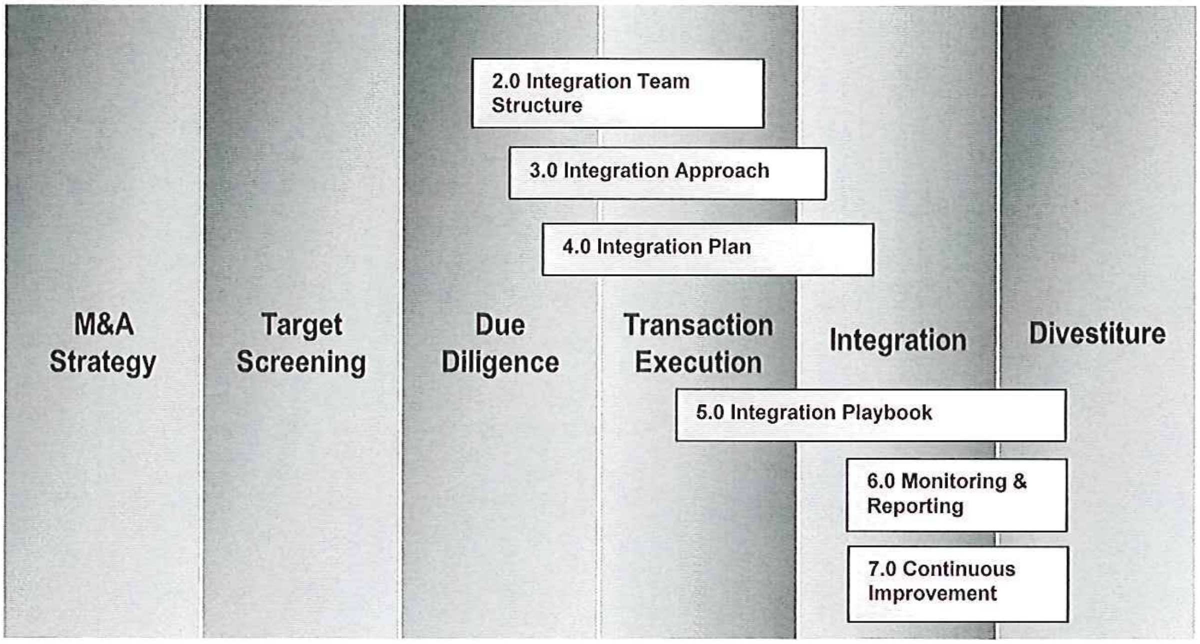
- Full-time Integration Leader
- Integration team structure
- Team member roles and competencies
- Talent identification

Governance

- Corporate Development Process Owner
- Steering Committee
- Integration team structure
- Monitoring and reporting
- Training
- Continuous improvement

1.7 Integration Guide Overview

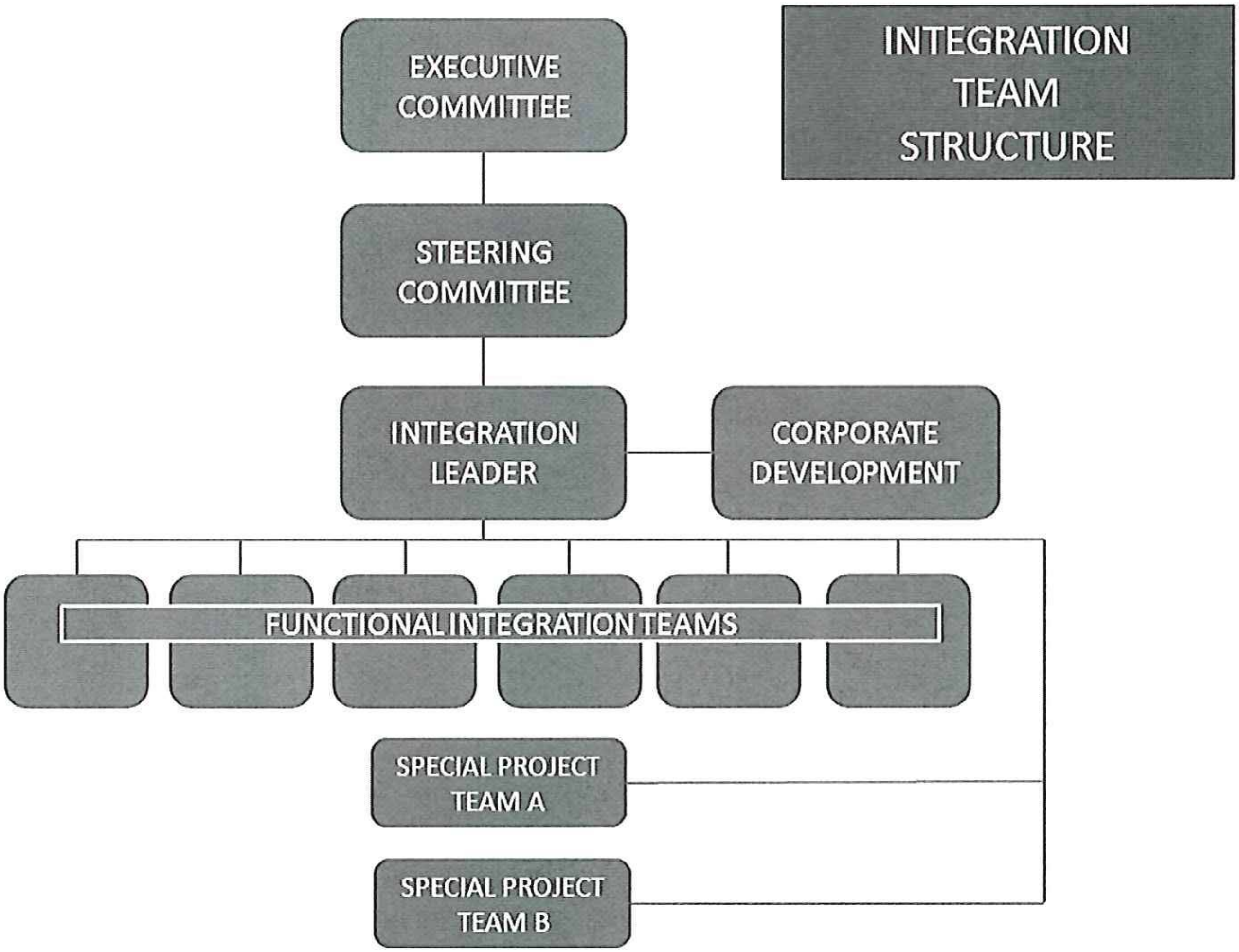
The following chart represents the relationship between the sections of the guide and the M&A lifecycle.



2. INTEGRATION TEAM STRUCTURE

2.1 Typical Structure:

The Integration Team Structure provides governance over the integration process and facilitates timely and thorough decision making. At the heart of the Integration Team Structure is the Integration Leader, who is accountable for integration execution. The structure also includes an Executive Committee, a Steering Committee, Corporate Development representatives, Functional Integration Team Leaders, Functional Integration Team Members, and Special Project Teams. Refer to Sections 2.2 through 2.7 for detailed roles and responsibilities of each member of the Integration Team.



Revision January 16, 2012

Association of Corporate Counsel

By in-house counsel, for in-house counsel.®

InfoPAK℠

Framework for Conducting Effective Compliance and Ethics Risk Assessments

Sponsored by:

corpedia

ETHICS. ELEVATED.

Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036 USA
tel +1 202.293.4103, **fax** +1 202.293.4701
www.acc.com

Framework for Conducting Effective Compliance and Ethics Risk Assessments

Updated August 2010

Provided by the Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, D.C. 20036 USA
tel +1 202.293.4103
fax +1 202.293.4701
www.acc.com

This InfoPAK^{SM} provides corporate counsel with an overview of the concept of risk assessment and to suggest useful practices for the handling of such in the corporate setting. It is based upon examination of more than a dozen leading organizations' risk assessment methodologies.

The information in this InfoPAK should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of Corpedia, Inc. or of ACC or any of their lawyers, unless so stated. Further, this InfoPAK is not intended as a definitive statement on the subject and should not be construed as legal advice. Rather, this InfoPAK is intended to serve as a tool for readers, providing practical information to the in-house practitioner.

This material was compiled by Corpedia, Inc. For more information about Corpedia, please visit their website at www.corpedia.com or see the "About the Author" section of this document.

Contents

I. Introduction and Overview

In an era of heightened expectations for proactive corporate governance, increased scrutiny under the Sarbanes-Oxley Act ('SOX'), and the major influence compliance practices have under the Federal Sentencing Guidelines for Organizations ("FSG"), institutions are increasingly looking to develop effective risk assessment procedures that: meet SOX and FSG requirements; prioritize compliance program initiatives and spending; provide a roadmap for improving compliance programs; reduce the likelihood of any material violations of federal, state and foreign jurisdiction laws and regulations; and demonstrate good-faith compliance efforts in the event of civil or criminal proceedings.

While the reasons for conducting a risk assessment are apparent, the overall process and methodology for developing and implementing them are less obvious. Common questions faced by those tasked with ethics and compliance include:

- How often should risk assessments be performed?
- Can the assessment process be performed internally or should an external third party manage it?
- How should areas of risk be prioritized, weighted, or ranked?
- Which internal stakeholders should be involved?
- What type of report should be generated and to whom should it be distributed?
- How should a risk assessment be conducted to provide a strong legal defense in the event of criminal or civil proceedings?
- What type of risk assessment will meet FSG criteria?

This InfoPAK, based on examination of dozens of leading organizations' risk assessment methodologies, will address these questions and assist in-house counsel in developing robust and effective risk assessment practices.

II. What is a Risk Assessment and Why is it Important?

"Risk" in this context is defined as an uncertain event or condition that, if it occurs, would have a positive, negative, or unclear effect on the entity in question. The key element of risk is its uncertainty, so in order to manage risk, organizations must proactively engage in a process where risks are identified and analyzed, and where a strategy is developed to mitigate them. This process is commonly known as "risk assessment."

It is important to note that risk assessment and its related activities may be considered elements of a larger risk management program. However, in this paper, we focus only on the specific role and associated processes of risk assessment itself, without discussing how to manage and mitigate risks once they are assessed and analyzed.

Broadly speaking, the actual components of a risk assessment are the following:[1]

- Risk Identification: determining which risks are relevant to the organization and documenting their characteristics.
- Qualitative Analysis: prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
- Quantitative Analysis: numerically analyzing the overall effect of risks on the organization.
- Defining Risk Appetite: determining the organization's risk appetite (whether financial, legal, operational, or reputational) in order to set compliance priorities.
- Risk Mitigation: developing options and actions to enhance opportunities and/or reduce threats to the organization.

A. Risk Assessment Goals

- The primary goals for organizations when completing an effective ethical and legal compliance risk assessment should be:
- To evaluate, quantify and prioritize legal and/or ethical misconduct and compliance risks specific to current organizational operations.
- To support arguments for planning and implementing robust compliance and ethics programs, including comprehensive training and oversight.
- To develop risk mitigation plans, including corporate policies and controls.
- To align an organizational compliance program with the Federal Sentencing Guidelines.
- To develop a benchmark for ongoing risk assessment and measurement of the program's effectiveness.

B. Rick Assessment Benefits

The accompanying benefits of conducting an effective risk assessment include:

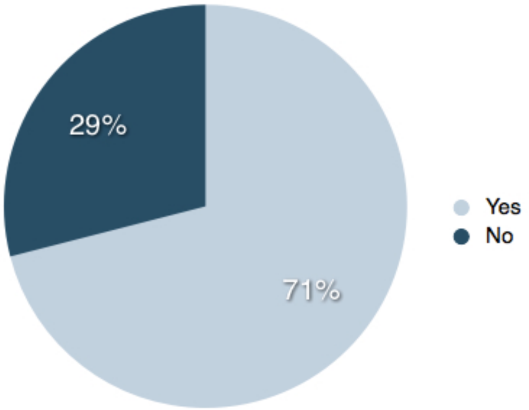
- Helping organizations prioritize compliance budget spending by identifying those areas most in need.
- Enabling the organization to modify and improve compliance program components, effectively reducing risk and decreasing the likelihood of criminal conduct.

Providing an affirmative defense to allegations of deficiencies in the design and administration of a compliance program, as well as any misconduct that does still occur. In fact, the Federal Sentencing Guidelines for Organizations explicitly state:

> *"In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.[2]"*

Given these benefits, more organizations are conducting periodic risk assessments. As illustrated in Figure 1, 71 % of all surveyed U.S.-based organizations conducted periodic risk assessments in 2009.

Figure 1 - Percentage of Organizations that Conduct Periodic Risk Assessments[3]



C. Compliance and Ethics Risk Assessment vs. ERM

The Enterprise Risk Management ("ERM") process focuses on market-created, systemic risks and includes an evaluation of operational controls, internal controls, and strategic planning. A compliance and ethics risk assessment focuses on people-created risks, such as risks resulting from personnel responsibilities. Many companies will often touch upon compliance and ethics-related risks as part of a broader ERM process, but fail to go into adequate depth.

III. Leading Practices

Organizations often face unique challenges in determining the necessary scope, frequency, and structure of their compliance and ethics risk assessment. However, as more organizations embark on compliance risk assessments and develop their methodologies, numerous leading practices have started to emerge. These practices, outlined below, offer organizations sensible guidelines for implementing their own effective and comprehensive risk assessments.

A. Examine All Major Areas of Potential Misconduct

An effective risk assessment examines all major areas of potential misconduct. A common mistake organizations make when conducting a risk assessment is limiting the potential universe of risks assessed to a preconceived short list of likely high-impact risks. However, a proper risk assessment considers the full realm of potential risks systemic to the average organization, as well as those that are unique to the industry within which the organization operates. A good assessment would seek to catalogue and examine risks involved in complying with every applicable federal, state, and local law or regulation. Additionally, a quality risk assessment would probe other ethics-related areas in which potential misconduct may adversely affect an organization's image and reputation.

B. Examine Risk Contextually

To achieve peak effectiveness, an assessment must include an examination of the controls, processes, and procedures designed to prevent compliance failure. Examining risks not only on their own, but also within the context of the organization's ability to plan for, prevent, or mitigate those risks, is crucial to properly prioritizing a response. Evaluating the capability of those in positions of substantial authority to recognize and prevent a compliance breakdown is also crucial.

C. Address Current and Potential Risks

An effective risk assessment considers both current issues and potential future risks. An assessment should not simply address risks that exist today, but also those that could reasonably develop in the future. For example, industry practices that are considered acceptable now could be called into question and cause issues later.

D. Industry Information and Historical Incidence Reports

Risk assessments should include an examination of industry information as well as historical incidence reports. Document review should not be limited to internal corporate documents; external documentation should be sought and reviewed as well. To be adequately predictive, an effective risk assessment should include not only "compliance breakdowns and failures," but "near misses" as well. This is particularly important when modifying the compliance program under the FSG requirements.

E. Participants From All Levels of the Organization

Effective risk assessments rely on participants from all levels of the organization. The leader of the risk assessment process should solicit the involvement of both functional leadership (e.g., sales, marketing, finance) and line leadership (e.g., division heads, executive team) in collecting and assessing potential risk areas. This is commonly achieved through workshops, focus groups, surveys, and interviews.

F. Judging Compliance Program Against FSG Benchmarks

In addition to assessing the organization's susceptibility to various compliance risks, an effective risk assessment will include a comprehensive review of the compliance program against the seven standards defined by the FSG. A comprehensive program review should gauge:

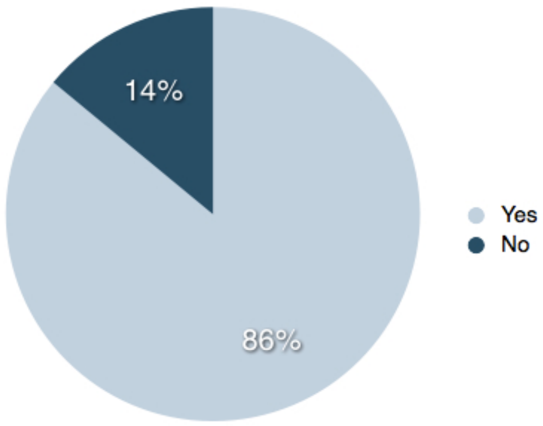
- Organizational culture of ethics and tone from the top
- Standards of conduct, internal controls, prevention and detection procedures
- High-level oversight, leadership accountability, resources and authority
- Due care
- Current training and communication programs

- Monitoring, auditing and whistleblower systems, risk assessment and program evaluations
- Enforcement and response

G. Impact and Likelihood of Occurrence

Risk areas should be weighted and ranked for their organizational impact and the likelihood of their occurrence. When conducting a risk assessment, the organization should assign quantifiable “likelihood” and “severity” weights or ratings to each relevant risk area. Utilizing this type of analysis helps organizations rank relevant risk areas from minor to severe impact and low to high chance of occurrence. This is becoming a more common trend among organizations; as Figure 2 illustrates, nearly 86 % of compliance professionals surveyed now analyze risk for both likelihood of occurrence and severity.

Figure 2 - Percentage of Organizations that Examine Risk by Both Likelihood and Severity in Risk Assessments[4]



H. Document the Outcome

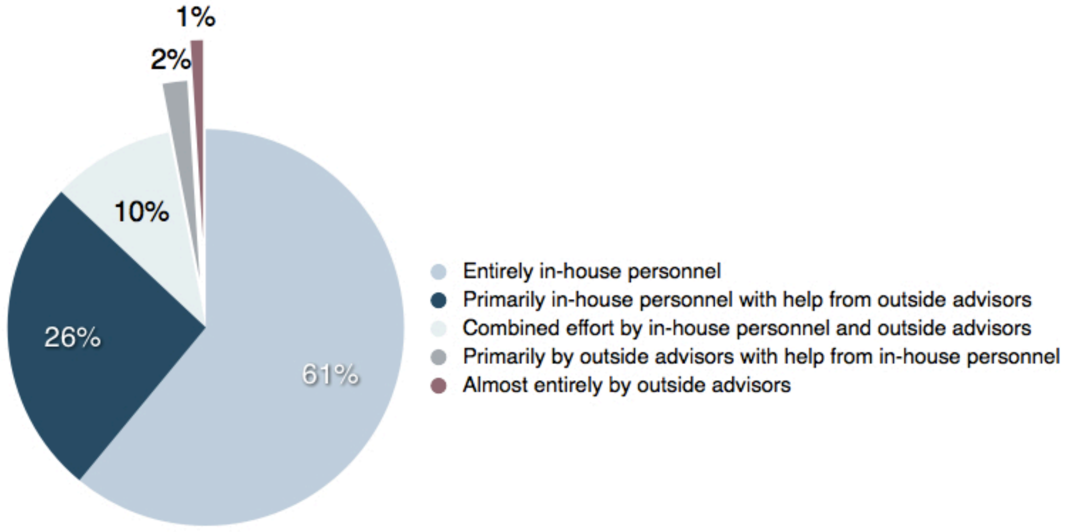
The organization should document the outcome of the risk assessment and convert the results into a defensible action plan. Good documentation may be introduced as an affirmative defense in the event of misconduct, demonstrating the existence of an effective compliance and ethics program. Such documentation should not only include the risk assessment process followed, but also the actions taken to design and implement a new compliance program or modify an existing one.

I. Be Defensibly Objective

The process methodology behind the risk assessment must be defensibly objective. This includes fairly assessing the full universe of potential risks, including existing acceptable industry practices. Organizations need to resist any temptation to ignore or deemphasize risks simply because they may be costly to address (either from a financial or internal political vantage point). To help ensure objectivity, an increasing number of companies are involving outside advisors in their assessments. As shown in

Figure 3, 39 % of all surveyed organizations currently involve independent outside parties to some extent when conducting risk assessments.

Figure 3 - Level of Involvement of Independent Parties in Compliance Risk Assessments[5]

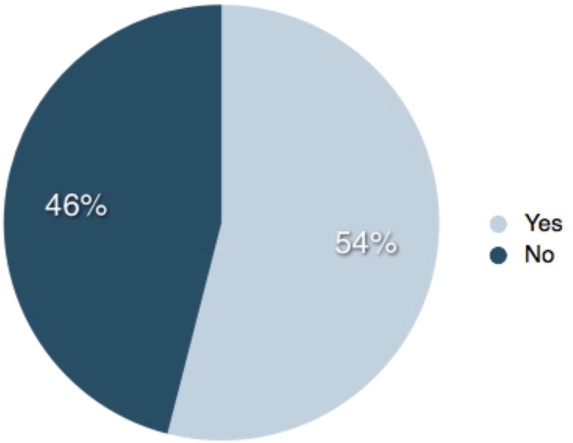


J. "Quantification" of Each Risk Area

The process by which the risk assessment is conducted should allow for a specific "quantification" of each risk area. An assessment that examines beyond mere "likelihood" and "severity" can be more useful in prioritizing compliance budget spending and activities. It can also justify any incremental controls, policies, processes, or costs needing implementation. Furthermore, if executed correctly, such quantification can be used to measure program effectiveness, another FSG criterion for compliance and ethics programs. As Figure 4 illustrates, over half of those surveyed (54 %) who say they conduct compliance risk assessments prioritize risks in a quantitative manner.

(Figure 4 on next page)

Figure 4 - Percentage of Organizations that Quantify Risk as Part of Risk Assessment Process Outcome[6]



K. Be Sufficiently Periodic

Risk assessments should not be a one-time activity. The frequency at which an organization chooses to conduct risk assessments and schedule follow-up reviews may depend on the nature of the organization's industry. However, if the methodology and process for the risk assessment is adequately defined, an assessment can easily be done on an annual basis. Operating environments, regulations, and government enforcement priorities routinely change, so it is inadvisable to conduct risk assessments less frequently than every two years. Furthermore, infrequent risk assessments are of less value in measuring the effectiveness of a compliance program.

L. Measure of Employee Knowledge

The risk assessment should include some measurement of employee knowledge and awareness of the compliance program and supporting controls. Most companies include employee knowledge and awareness as a measurement factor in their risk assessments.[7] Doing so helps pinpoint the areas in which communications and training programs need to be improved. One of the most common methods of accomplishing this is through simple online employee surveys.[8]

M. Benchmarking

The risk assessment should benchmark against peer organizations. If it is feasible and such information is accessible, companies should compare their risk areas and compliance program activities to others within their industry or other companies that share a similar size and operational profile. This is particularly important, as it ensures the organization conforms with "accepted or applicable industry practice" as outlined in the application notes to the U.S. Federal Sentencing Guidelines Manual.[9] Although a company potentially could even reach out directly to a competitor to conduct a benchmarking survey, this is inadvisable due to antitrust concerns. Another resource used by organizations for benchmarking data is Corpedia's ECERA™ (Enterprise Compliance and Ethics Risk Assessment) database, which catalogs hundreds of organizations' compliance programs.[10]

N. Coordinating with Internal Audits

It is common and often quite useful to coordinate the risk assessment with internal audits. These days, more companies are taking steps to increase coordination between the internal audit and ethics and legal compliance risk assessment. After all, risk assessments are used to identify, measure and rank risk areas. Completion of an assessment produces the following results for the internal audit:

- Aligns company focus and resources to address areas of greatest significance to the organization.
- Allows the auditor to design a program that tests the most important internal controls.

Using information from one in the preparation for the other is both acceptable and recommended. However, the organization must never confuse the primary purpose of either and the associated analysis must be kept separate and distinct. Remember, an internal audit focuses primarily on internal controls and financial risks, whereas an effective risk assessment will look at a much broader universe of compliance and ethics risks (such as employment law, antitrust, environment, safety, health, trade compliance, privacy, etc.).

IV. Major Universal Characteristics of an Effective Risk Assessment

Before commencing your risk assessment, it is important to understand some of the key characteristics of an effective risk assessment's design. Though every organization's risk assessment will be slightly different, all should strive to include these qualities, which will help ensure that the assessment will capture and measure all risks, both apparent and unforeseen. Additionally, they provide a framework for a repeatable process that can be used to plan and improve any compliance program.

A. Flexibility

When undertaking a risk assessment, organizations naturally attempt to catalogue a portfolio of potential risk areas. While this risk portfolio may be independently derived, the organization may also leverage an external resource (for example, a risk database that bears information on common risk areas). Regardless of how comprehensive a "risk universe catalog" appears to be, a good risk assessment process is flexible enough to allow the addition of new or unforeseen risks.

New risk areas may be identified by the risk assessment team, advisory councils, business leadership, or employee surveys, or may arise through an "alternative interpretation" of a catalogued risk that needs to be addressed. For example, given increased awareness and sensitivity to compliance and corporate governance, it is not unusual for established, commonly accepted business practices in any industry to attract new scrutiny, leading to new regulation or reputational damage.

B. Measure and Rank Risk by Impact

Not all compliance failures that could result in violations of the law are equal. Some "material violations" may result in fines or penalties on top of substantial legal defense costs, while others may significantly affect an organization's operations, causing substantial customer and contract losses, reputational harm, or even requiring substantial changes to the business model. The impact of various compliance failures by area or category of risk depends on the industry in which an organization operates, historical incidence of compliance failures, and judicial enforcement trends. A good risk assessment will consider the resulting impact of any risk found and weigh risks based on their impacts.

For instance, OMB Auditing Standard 133, which translates the internal control deficiencies defined in SAS 112 into compliance terms, is useful for standardizing and comparing compliance risks.[11] The compliance risk assessment should also define standard "risk appetites" across risk areas (financial, operational, legal and reputational) so that different risks may be objectively compared.

C. Standardized and Documented

A common flaw in organizations' risk assessment efforts is for the assessments to be treated as a one-time event and hence fail to be sufficiently documented or consistently improved. The FSG criterion for an "effective compliance and ethics program" supplies the expectation that risk assessments are a recurring activity within an organization's overall compliance program. A well-designed risk assessment has a systematic methodology and well-documented process, and therefore is more likely to meet objectivity standards. Objectivity is a major concern for organizations, as any subjective bias imputed by those conducting the risk assessment (particularly if they are internal personnel) can undermine the credibility of the final product.

Documented, standardized processes allow for more cost-effective repetition of the risk assessment processes. Inevitably, endemic change occurs both within the organization and the business environment in which it operates (e.g., through new laws or reinterpretations of existing laws; compliance and legal departments experience personnel turnover; organizations divest operations or enter into new business activities or markets), and new risks resulting from these changes must be proactively assessed and handled. Additionally, with a sufficiently standardized and documented process, a risk assessment can measure the effectiveness of an organization's compliance and ethics program development by comparing outcomes over a series of sequential risk assessments. Finally, maintaining substantial documentation and a standardized process can make an organization's risk assessment procedure easily defensible if necessary.

D. Enterprise-Wide

Limiting a risk assessment to only part of the organization, such as specific geographic regions or unique functional areas, can leave the organization open to exposed risks. In recent years, some of the most costly compliance failures (in terms of out-of-pocket losses and reputational damage) for U.S. organizations have occurred overseas. While it is tempting to focus an assessment on those areas with which the legal department is most familiar, doing so would undermine the effectiveness and defensibility of the analysis.

E. Distinct from Sarbanes-Oxley § 404 Assessments

While correlations certainly exist between work performed by the internal audit function of any organization and a risk assessment undertaken by the compliance, ethics, and/or legal departments, these analyses must still be kept separate and distinct. Sarbanes-Oxley § 404 requires management to document and assess the effectiveness of their internal controls over financial reporting.[12] Additionally, new guidance from the SEC permits organizations to use a risk prioritization approach when conducting their § 404 work in the future. Such risk prioritizations have the potential to interlay with risk assessment; however, the fundamental elements examined under § 404 are very different from an assessment of risk areas (e.g., the effectiveness of processes and procedures to detect *actual* material violations of law, rather than the *probability* of violations), and accordingly these analyses should remain separate.

In short, "risk" from the perspective of an internal audit is fundamentally different from "risk" as assessed by the legal compliance function. Utilizing information from one analysis or assessment in the preparation of the other is both admissible and encouraged. However, these are not identical types of "risk," so allowing the two to become interchangeable is a mistake. While internal auditors may participate in, or possibly even lead a legal compliance risk assessment, the risk assessment must be sufficiently individualized and distinct from the material disclosure work done for Sarbanes-Oxley § 404.

However, the assessment of internal controls conducted in the course of a § 404 audit can be implemented effectively as part of the risk assessment, and vice versa. Many companies successfully employ the Committee of Sponsoring Organizations of The Treadway Commission ("COSO") methodology[13] when conducting internal control surveys, including surveys of internal compliance controls and their potential impact on financial statements. A compliance risk assessment can be aligned with an internal audit by using COSO methodology to conduct broader compliance risk analysis, which requires an assessment of internal controls.[14] Under The Public Company Accounting Oversight Board Audit Standard #5, management can use an independent assessment of internal compliance controls to support their annual certifications.[15] Conducted properly, compliance risk assessments can effectively serve this dual purpose. Those conducting the risk assessment, however, must pay close attention to ensure that risks are assessed from both internal audit and risk assessment perspectives.

V. What to Examine in a Risk Assessment

A. Risk Severity

When conducting a risk assessment, the organization should assign quantifiable "likelihood" and "severity" weights or ratings to each identified risk area. There are numerous resources, both internal and external, that prove extremely useful in determining the likelihood and severity of any given risk. When looking at the severity of risk, a good approach is to compute the maximum potential severity (the "worst case scenario") should a particular type of misconduct occur. While innumerable elements can drive risk severity, listed below are some of the most common factors to be considered:

- Civil and criminal penalties potentially resulting from violations.
- Legal defense costs.
- Litigation settlements.
- Impact on revenue and earnings.

- Impact on stock value.
- Impact on credit rating and cost of capital.
- Employee turnover.
- Customer loss.
- Change in business model and operations (such as shutdown of various business operations or product or service lines).
- Debarment from participation in government contract or grant programs.
- Change in market share.
- Reputational damage.
- Negative media coverage.
- NGO/advocacy group pressure.
- Increased future costs of compliance.
- Current and anticipated regulatory initiatives and enforcement/prosecution priorities.

Most organizations lack sufficient internal data or incident-related experience to accurately determine the severity of risk areas under examination. However, industry experience, as well as broader corporate experience, can provide adequate information for reasonably accurate analysis of risk severity. A number of studies exist that statistically measure the severity of various risk areas for major industries.

B. Risk Likelihood

It is important to note that, while an accurate understanding of risk severity is critical, there is little an organization can do to reduce that severity. What the organization can do, however, is reduce the likelihood of the risk itself. Therefore, an accurate assessment of risk likelihood and a solid understanding of the underlying factors are paramount to any good risk assessment methodology.

"Risk likelihood" is a combination of internal factors which determine the probability that a particular type of misconduct will occur. The following major factors affect—and indeed create—the risk probability:

- Business activities
- Policies, procedures, processes, and controls
- Organizational culture and ethics
- Employee knowledge, awareness, and intent
- Below is a sample of key tools and activities organizations can utilize to aid the risk assessment process:
- Executive interviews and focus groups.
- Organizational health surveys.
- Employee awareness/knowledge assessments.
- Examination of corporate policies, processes, and controls per risk area.

- Examination of the anonymous reporting system statistics.
- Review of other historical incidence.
- Evaluation of existing training inventory and courseware.
- Interviews with training "owners."
- Examination of prior audits, surveys, and reports.
- Review of corporate publications (code of business conduct, employee guides, new hire kits, etc.).
- Examination of organizational charts and reporting relationships.
- Review of Audit Committee Charter and Corporate Governance Principles.
- Assessment of employee disclosure and acknowledgement forms.
- Analyst reports.

VI. The Ten-Step Risk Assessment Process

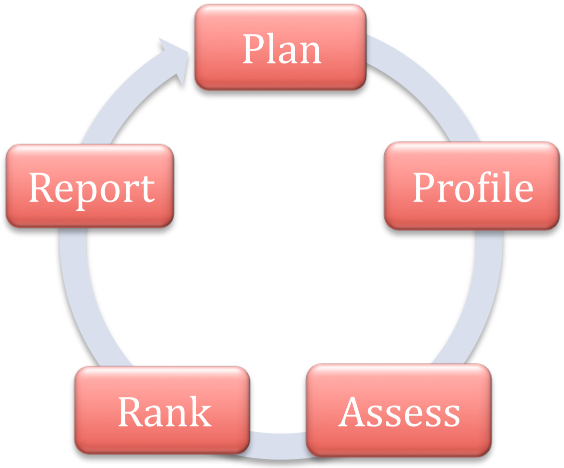
The ten key steps in an effective risk assessment process are as follows:

- Definition of Objectives, Criteria and Documentation
- Planning the Process
- Profile the Organization
- Catalog Risk Area Universe
- Rate Risk Areas for Severity
- Conduct Interviews, Surveys and Assessments
- Catalog and Measure Mitigating and Aggravating Factors
- Determine Risk Event Probabilities or Likelihood
- Determine Aggregate Risk Scores (Enterprise Impact) and Final Ranking
- Finalize Risk Assessment Report and Create Mitigation Action Plan

This process represents an amalgamation of best practices and methodologies employed by leading organizations that Corpedia has either observed or worked with via prior engagements. Depending on resources and facilities with risk analysis, some companies may eliminate or combine certain steps. Others may wish to add incremental steps, such as peer analysis and benchmarking.

Although your organization may deviate from these steps, the fundamental sequential principles remain the same in any effective risk assessment. These principles include planning, profiling, assessing, ranking and reporting.

Figure 5 - Risk Assessment Process Grid



A. Step One: Definition of Objectives, Criteria, Process and Documentation

The first step in commencing a risk assessment is to define the process. The proposed methodology must be specific to the desired outcomes and supporting processes for communication and handling documentation. These are the critical questions that need to be addressed when defining the risk assessment process:

- What is the desired outcome?
- Who is the target audience for the final report?
- How will this report be used?
- How will the organization manage the documents to be created?
- How will the issue of "privilege" be addressed?

1. Desired Outcome

For most, the practical purpose of a risk assessment is to meet the FSG criteria for an "effective compliance and ethics program." Taking this a step further, a risk assessment should reaffirm the emphasis on an existing compliance program or serve as an impetus for the creation of a new program where none exists. Knowing the parameters of the outcome may sound simple, but answering the above questions will determine the scope, depth and breadth of your risk assessment. For example, if the goal is to reaffirm the priorities of an established program, then the risk assessment might focus primarily on the risk categories and areas already contained and set forth in your organization's Code of Conduct. In the absence of a mature compliance program, and in order to use the risk assessment for purposes of budgeting and building a new or reestablished compliance program, it is preferable to:

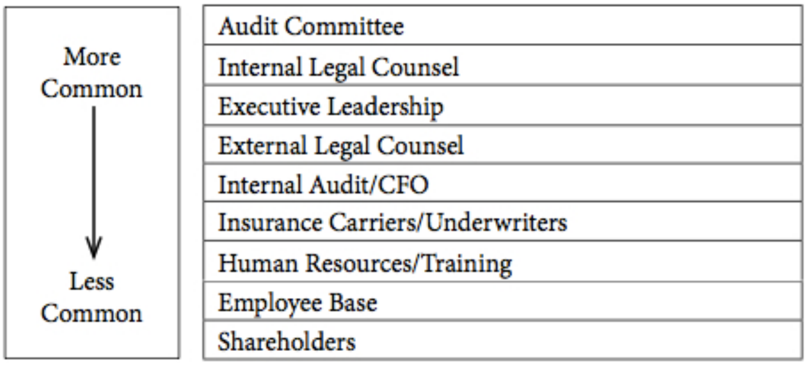
- Examine a far greater range of risk areas.
- Research what peers of similar size or industry are doing.

- Broaden the scope of the risk assessment team to include key functional areas and business leaders.

2. Target Audience

Understanding the target audience—or audiences, as there may be several—of a risk assessment will better prepare an organization for the type of data that needs to be collected in the assessment itself. In our experience and in reviewing leading organizations' risk assessment reports, some common target audiences include those featured below:

Figure 6: Target Audiences for the Risk Assessment



Audit Committee
Internal Legal Counsel
Executive Leadership
External Legal Counsel
Internal Audit/CFO
Insurance Carriers/Underwriters
Human Resources/Training
Employee Base
Shareholders

3. Use of Report

The report can be used to address/support:

- Policy and process creation.
- Training initiatives.
- Sarbanes-Oxley § 404 work prioritization.
- Purchase of incremental insurance.
- Divestment of product lines, customers, or markets, etc.

4. The Issue of Document Creation and Privilege

Completing a risk assessment can be very beneficial when delivered properly. However, organizations should be aware that a poorly executed assessment might compromise the sensitive information collected as part of the risk assessment and can potentially subject the organization to harm. One of the most vexing tasks of any legal department conducting a risk assessment is ensuring that the form, content and tone of any document created by the risk assessment team does not subject the organization to any unintended harm. The assumption that all created documents are protected by attorney-client or work product privilege is dangerous, as many documents may fall outside of the established privilege parameters in how they are generated or shared.

Privilege is very hard to maintain in today's legal environment; its veil is commonly pierced through waiver in regulatory and judicial investigations. In light of these issues, many corporate counsel adopt an operating assumption that privilege is unreliable or of limited use.

Any risk assessment will contain lists, descriptions and theoretical suggestions about current or possible future compliance problems. For example, envisioning "what could go wrong" is a useful exercise in helping to prevent such an occurrence. At the same time, should such a compliance problem later occur, written documentation from the assessment could be taken out of context as "evidence" of preexisting knowledge of a compliance problem or deficiency that an organization failed to address.

An additional complication is that an effective risk assessment commonly includes a diverse team of individuals, including both employees and non-company personnel. It is likely that the majority of these individuals will not be attorneys, and many of them may not be knowledgeable about the concept of privilege and the associated dangers of document and content creation. Furthermore, some of these individuals, intending to grandstand about their participation in the project, can lend themselves to dramatic verbiage and overstated pronouncements about potential risk areas in their documentation creation. As a result, guidelines and protocols for document creation should be established for the risk assessment team and any other key contributors. At a minimum, documentation guidelines should include the following:

- Detailed Guidelines for Content and Language: Guidelines should focus on counseling participants to be clear and accurate in their writing, use neutral language, and avoid hyperbole and exaggeration. Participants should also understand that any document might be taken out of context and to structure their writing accordingly. Furthermore, participants must apply these same guidelines to shorthand, margin, and handwritten comments and notes.
- Limitations on Document Distribution: Naturally, the broader the copy and distribution of drafts and documents, the greater the risks of losing control over what exists. Clear parameters should be defined for document submission and storage.
- Provide Guideline Templates: Should participants take part in ranking risks and creating hypothetical situations, it is best to provide a descriptive template with which they should work.

B. Step Two: Planning the Process

Once the organization has clearly defined the purpose, process, and desired outcomes of the risk assessment, it is important to map out a plan for executing the process.

1. Appoint a Risk Assessment Leader

As is important for any new endeavor, a leader must be selected to oversee the risk assessment process. Depending on the organization, this individual could be drawn from any number of roles, including general counsel, chief compliance officer, ethics officer, head of risk management, or the director of human resources. It is also possible for this leader to be suggested or appointed by any of the individuals listed above. Regardless of level, the leader of the risk assessment process must be empowered to control the process throughout – from inception through final implementation.

2. Identify and Select Team Members

The success of the leader is contingent upon the effectiveness of their team. As such, it is important to identify key individuals in the organization who will serve as members of the risk assessment team. Some of the more common members include:

- General Counsel and/or Chief Compliance Officer
- Legal and/or Compliance Subject Matter Experts
- Business Unit or Functional Heads
- Outside attorneys or consultants (as necessary)

When selecting team members, it is imperative that they understand the purpose and process of risk assessments and have substantial knowledge of the relevant business units and functions being observed.

3. Decide Which Steps to Include/Perform

Each organization is unique and therefore is likely to be at a different stage or maturity level in terms of conducting risk assessments. Novice organizations currently implementing or planning to implement a risk assessment for the first time would be advised to complete each step methodically and carefully, while other more experienced entities that have completed multiple risk assessments may decide to streamline their process.

4. Will You Quantify Risk or Just Write a Qualitative Report?

Another determination the organization must make is whether the portfolio of risks will be quantified or assigned a value based on their potential impact on the organization, as well as the likelihood of their occurrence. The value of conducting a risk assessment is the ability to measure the degree to which a specific risk can affect the organization, either positively or negatively. Positive risks present opportunities for the organization, while negative risks naturally serve as potential threats. Depending on the type of organization and its associated industry, the number of potential risk areas for the organization can vary. As such, the quantification of risk areas provides a mechanism to allow for the ranking of risk areas.

Based on recent research, many companies still decline to quantify their risk areas and instead rely on a more subjective, qualitative analysis where they base their risk assessment and corresponding mitigating strategies on opinions and feedback from personnel in their organization. As illustrated in Figure 4, only a little over half (54 %) of all organizations actually quantify risk in their risk assessments.

5. Will You Be Conducting Workshops?

Some organizations choose to conduct group meetings or workshops to identify, evaluate and prioritize risk areas. These meetings, managed by the risk assessment leader with the aid of the risk assessment team, examine all of the relevant risks to the organization, assigning scores to each risk for their severity and likelihood. Whether or not the workshops will prove productive depends heavily on the organization. In order to achieve productivity, it is important for the risk assessment leader to manage the process fully. This includes selecting the right participants, defining guidelines and expectations for the workshops, providing sufficient background material and guidance, and creating an effective schedule and agenda for the meeting.

6. Will You Be Conducting an Employee Survey?

In the past, when conducting risk assessments, some firms have chosen to exclude the broad employee base and instead focus their risk assessment queries on key functional areas and business leaders of the organization. In fact, recent research conducted by Corpedia and the Association of Corporate Counsel found that less than 14 % of organizations actually use workforce surveys as part of the risk assessment process.[16] Taking the time to perform an employee survey can help protect the organization from prematurely dismissing or failing to recognize certain risk areas. It is quite common, especially in highly decentralized organizations, for information gaps and communication failures to exist. As such, including an employee survey as part of the overall risk assessment will lessen the chance of omitting a key risk area.

7. Will You Be Conducting Interviews?

Some organizations will include interviews with department heads and executive leadership as a part of the risk assessment process. Getting a clear sense of what keeps those responsible for various business units or functional groups “up at night” can provide insight as to where compliance gaps may lie. Other areas of interest include:

- What key ethics and compliance issues are faced by the individual’s function? Business unit? Enterprise wide?
- Are the necessary compliance policies and procedures in place? Are they effective? Is ethics training provided to employees at your location or business unit?
- What is leadership doing in the individual’s location or business unit to establish a credible tone from the top? Are ethics and compliance emphasized throughout? What is the individual’s perception of the overall tone from the top?

Individuals leading international locations and various function leaders (sales, most commonly) are usual candidates when conducting interviews.

8. Estimate Resources

When planning the scope of the risk assessment, the resources necessary must be determined. This includes estimations of how much time is required of those resources, as well as verification of their availability. It is important for all participants of the risk assessment to make an honest and effective contribution to the process. Given the importance of the risk assessment to the organization, any weakened participation can lead to holes in the overall effort.

A major component of resource identification and planning is the decision of whether to conduct the risk assessment entirely in-house or to partner with an external party or advisor (law firm, audit firm, etc.). The costs and benefits of such a decision are discussed in more depth in Section VII: In-House vs. Outsourcing the Risk Assessment.

9. Set Milestones

An effective risk assessment involves a significant number of interrelated tasks necessitating the active involvement of many individuals. Depending on the actual number of risk areas assessed, the process can quickly become quite complicated. As such, it is important for the appointed leader of the risk assessment to set specific, measurable goals and checkpoints throughout the process. The use of milestones will help guide individual contribution, as well as establish a structure for a process with multiple diverse inputs.

C. Step Three: Profile the Organization

Once the planning stage reaches completion, the next step is to develop an accurate profile of the organization. This step is not to be underestimated, as it effectively drives the rest of the risk assessment process. Moreover, diligence and care are required when performing this step of the process. A company's profile dictates the types of risk areas relevant to the organization; a weak or inaccurate profile will lead to an ineffective risk assessment.

Some of the typical elements addressed in a company profile include specifications of the organization in the following areas:

- Industry type
- Company size
- Classification (public versus private)
- Key aspects of business operations (e.g., consumer products, government contracting, union environment, etc.)
- International operations

Profiling the organization involves comprehensively reviewing its business activities, strategy and priorities, industry and geography of operations, workforce composition, and other operational circumstances that generate exposure to particular risk areas.

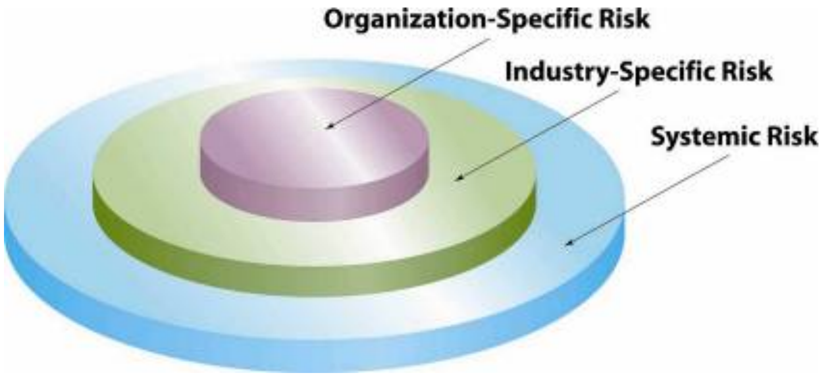
D. Step Four: Catalogue Risk Area Universe

Completing the organizational profile enables the development of a complete catalog of risks, commonly known as a risk universe. Although organizations are exposed to an incredible variety of risks threatening the business itself on a daily basis, such as sudden schedule, budget, or quality constraints hampering the delivery of a product or service, our analysis focuses specifically on ethics and legal compliance risks–that is, those risks related to the potential for business misconduct and/or violations of federal, state, and/or local laws and regulations. A robust risk assessment process attempts to map out every business process of the organization and the ethics and compliance risks associated with each. This process would ideally be repeated annually and serves as the foundation for conducting a risk assessment.

1. Tips

When developing the risk universe, it is necessary to adopt a comprehensive view. The organization must strive to first identify and scrutinize risks, pinpoint their root cause, and then widen the examination to account for systemic risks (common to the average organization), industry-specific risks and finally, organization-specific risks. It is also useful to rely on the experience of peer groups and review historical incidence.

Figure 7 – Risk Universe



It is useful to display the entire set of risks in an Excel grid format, enabling risk assessment leaders or team members to capture, sort and rank the risk areas later in the process, once they have been rated for severity and likelihood of occurrence. An example of this type of grid is available in Section XI, Sample Forms.

E. Step Five: Rate Risk Areas for Severity

Once the risk universe is fully developed and all relevant risk areas to the organization have been identified, the next step in the process is to rate those risk areas for severity.

Risk event severity is a product of many factors including:

- Civil/criminal penalties, such as SEC/DOJ settlements, lawsuits, etc;
- Impact on stock price and bottom line;
- Employee turnover and loss of intellectual property;
- Loss of customers and market reputation;
- System business model impact;
- Increased future cost of compliance;
- Current and anticipated future enforcement trends and priorities.

1. Rating System

Risk areas can be rated for severity both subjectively and statistically. A subjective scale will typically characterize the level of a risk from minor to moderate to severe impact, while a statistical scale will rely on a numeric rating or weight assigned to the risk. The scale can vary but is often simply a range of either 1-5 or 1-10 where the level of severity is ranked in ascending order. Often, once the risk likelihood is calculated, organizations process both data sets and visually map them on a probability-impact matrix. An example of this matrix is available in Section XI, Sample Forms.

2. Leverage Peer Data

When evaluating the complete portfolio of risk areas for impact to the organization, one may find it helpful to research available benchmark information on how their industry peers rate or have rated specific risk areas to their organizations. When benchmarking, it is important to choose one or more peer organizations that closely match the subject organization in terms of size and industry type, among other factors.[17]

Another alternative is to design a customized industry peer survey and distribute it among a selection of peer organizations in order to obtain common severity metrics. However, this process may be considerably lengthy and requires effective planning and design by the host organization. Some companies opt to develop an internal database of news items from multiple media sources, identifying potential or actual risks relevant to those companies so they will be "remembered" at the time of periodic risk assessment.

F. Step Six: Conduct Surveys, Interviews, Document Review, and Program Assessments

The next step in the process is to collect information that will enable determination of the likelihood of misconduct with sufficient accuracy. This step typically involves conducting interviews and/or assessments with senior and mid-level managers, key functional area leaders of the organization (e.g., department heads in finance, sales, etc.), and potentially a sample of the workforce. A secondary goal of this research is to verify the integrity of the risk area universe constructed earlier, and discover any material risk areas that may be missing from it. Sometimes, interviews with those "at the front lines" can uncover totally unforeseen yet material risks.

1. Surveys

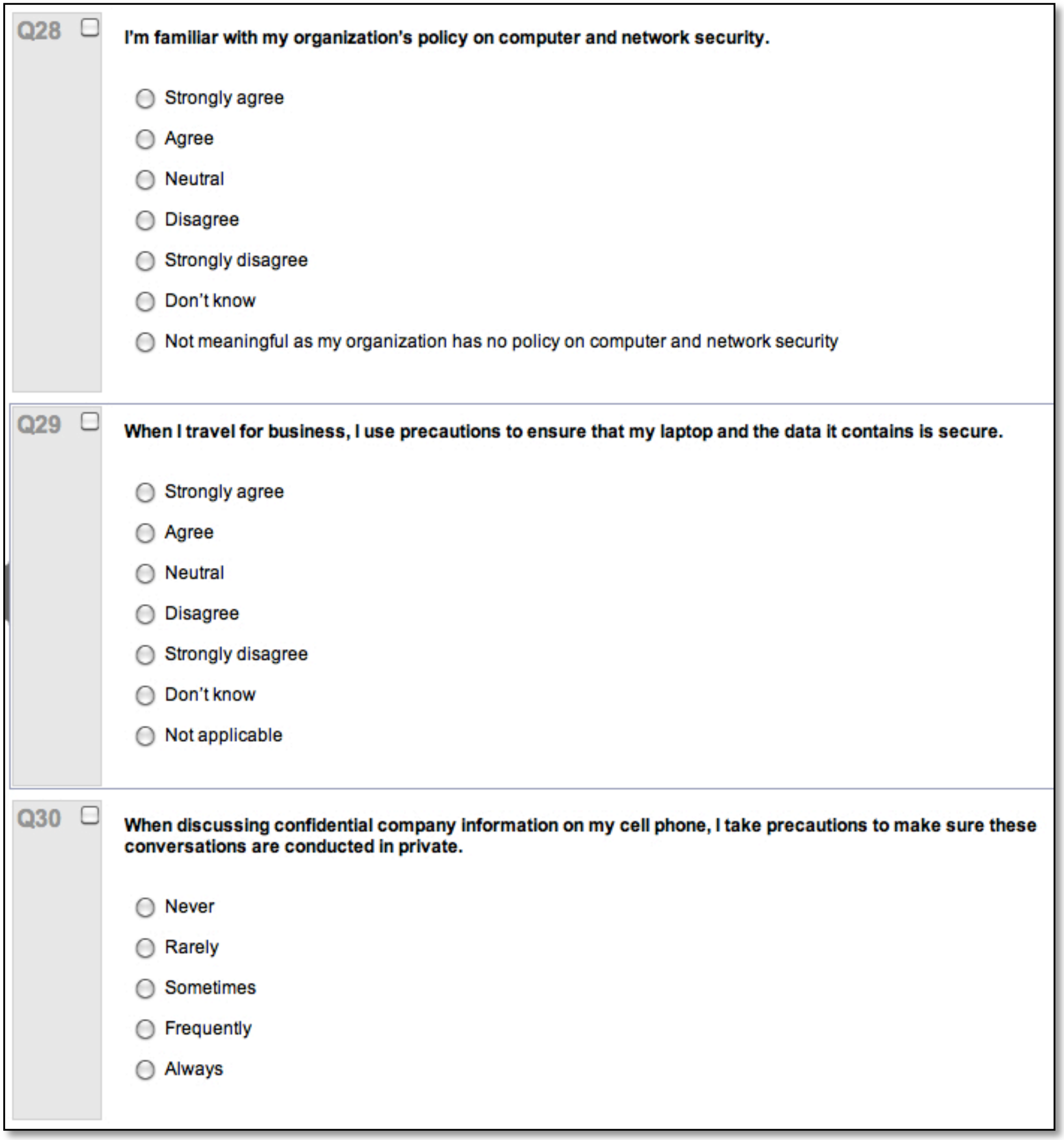
As with any organization, plant and/or field employees are the first line of defense in detecting and reporting any business misconduct or unethical behavior. As such, it is imperative that all levels of employees be included in the assessment of compliance risk.

The most common (and cost effective) method of gauging the organization's ethical health and employees' level of compliance knowledge is through the use of employee surveys. When conducting surveys, two general types of survey assessments can be utilized: (1) Compliance Environment Assessment and (2) Employee Culture and Compliance Knowledge Assessments.

Compliance Environment Assessments evaluate organizational policies, processes, procedures and controls, historical incidents, the quality and extent of existing compliance efforts, existing ethics/compliance training programs, current compliance issues, corporate culture (as viewed by senior management), business priorities, an evaluation of the overall compliance and ethics environment, and corporate commitment to ethics and compliance. While some components of the Compliance Environment Assessment can be examined through comprehensive analysis of existing data—such as the training curriculum, code of conduct, management communications, written policies, internal audits, reporting hotline statistics, and prior surveys—a significant portion of data is collected through targeted surveys, questionnaires and interviews. Figure 8 provides a snapshot of a typical Compliance Environment Assessment.

(Figures 8 on next page)

Figure 8 – Sample Compliance Environment Assessment



Q28 □ **I'm familiar with my organization's policy on computer and network security.**

○ Strongly agree
○ Agree
○ Neutral
○ Disagree
○ Strongly disagree
○ Don't know
○ Not meaningful as my organization has no policy on computer and network security

Q29 □ **When I travel for business, I use precautions to ensure that my laptop and the data it contains is secure.**

○ Strongly agree
○ Agree
○ Neutral
○ Disagree
○ Strongly disagree
○ Don't know
○ Not applicable

Q30 □ **When discussing confidential company information on my cell phone, I take precautions to make sure these conversations are conducted in private.**

○ Never
○ Rarely
○ Sometimes
○ Frequently
○ Always

On the other hand *Employee Culture and Compliance Knowledge Assessments* assess both organizational health and individual knowledge. They seek both broad impressions of the organization in regards to the ethics and compliance environment, culture, and overall ethical health, and employee comprehension of compliance issues with respect to their specific functional area.

Compliance knowledge survey questions are best presented as scenario-based, multiple-choice questions that test a respondent's knowledge of a specific compliance issue, while topics appropriate for an effective employee culture assessment include:

- Awareness of the organizational code of conduct.
- Perceived ability to recognize misconduct.
- Perceived ethics of executives, supervisors, and coworkers.
- Perceived tone from the top.
- Prior observations of misconduct.
- Willingness to report misconduct (including the reasons why or why not).
- Awareness of resources to ask questions or report misconduct.
- Perceived non-retaliation.
- Awareness of disciplinary mechanisms.

2. Interviews

For organizations that conduct employee interviews as part of the risk assessment process, the three most common groups to be interviewed are: senior management (including department and business unit heads), middle management, and the executive team.

Effective interviews will inquire into what the interviewee perceives as pressing compliance and ethics issues, from both a function or business unit perspective and an enterprise-wide perspective. These interviews also inquire into the perceived effectiveness of existing compliance policies and procedures, as well as the perceived quality of existing compliance training and communication initiatives.

3. Document Review and Program Assessment

A thorough evaluation of an organization's current compliance program is an integral component of an effective risk assessment. It is important to evaluate both enterprise-wide and centralized program elements and specific regional or country aspects. A robust program review will take into account:

- Written standards, including the code of conduct, policies, and procedures.
- Compliance program structure, responsibility, and oversight.
- Current training and related communication initiatives.
- Internal controls, monitoring, and auditing (including due diligence/venting practices, contractual provisions, certifications and disclosures, compliance tracking and auditing practices, accounting provisions).
- Enforcement and discipline.

A comprehensive review of written standards and related compliance documents encompasses internal and external documentation relevant to an organization's program effectiveness, including an examination of:

- Code of conduct
- Policies and procedures
- Reporting hotline statistics, investigation reports, and relevant disclosures

- Organizational charts and reporting relationships
- Disclosure and certification forms
- Documented training curricula and resource inventory
- Internal audit reports
- Third-party auditor and analyst reports
- Corporate reviews, awards, ratings, etc

G. Step Seven: Catalog and Measure Mitigating/Aggravating Factors

The next step of the process involves identifying specific factors relevant to the organization that can either reduce or increase the level of risk for the organization. Recall that this information is derived from the internal and external factors originally examined in earlier stages of the risk assessment.

H. Step Eight: Determine Risk-Event Probability or Likelihood

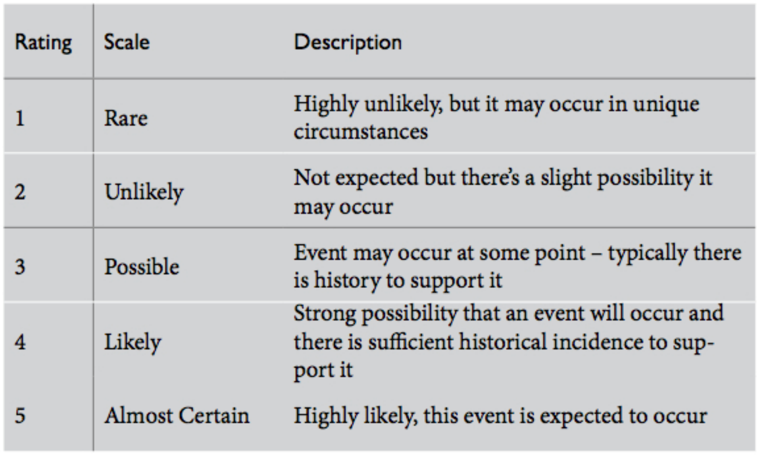
Information gathered during interviews, surveys, and assessments helps accurately determine the "risk likelihood" or the reasonable likelihood of the risk event occurring. Risk likelihood is a product of mainly internal organizational factors, including:

- Organizational culture and ethics
- Compliance initiatives
- Organizational policies
- Internal controls
- Workforce awareness and knowledge
- Employee intent.

For the actual scale used, it is common to use a scale of 1-5, as seen in Figure 9 below:

(Figure 9 on next page)

Figure 9: Risk Likelihood Scale Example

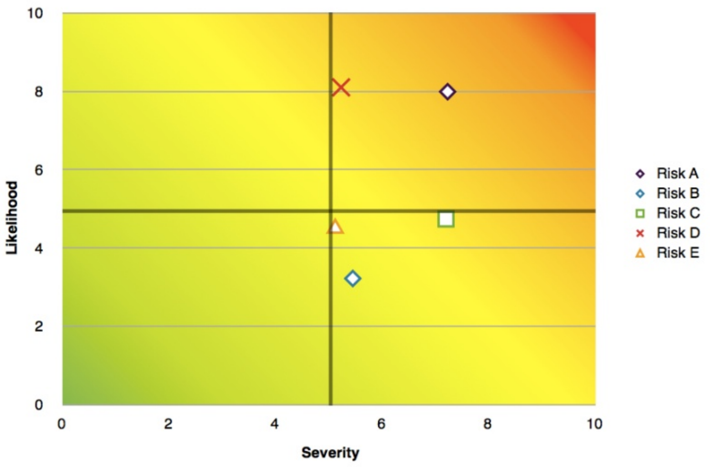


Rating	Scale	Description
1	Rare	Highly unlikely, but it may occur in unique circumstances
2	Unlikely	Not expected but there's a slight possibility it may occur
3	Possible	Event may occur at some point – typically there is history to support it
4	Likely	Strong possibility that an event will occur and there is sufficient historical incidence to support it
5	Almost Certain	Highly likely, this event is expected to occur

I. Step Nine: Determine Aggregate Risk Scores and Final Ranking

Once the severity and likelihood of each risk is known, an aggregate risk score (or Enterprise Impact Score) can be developed. This risk score, essentially the product of severity and likelihood, reflects the significance of a particular risk area to the organization. It is important to note here that this aggregate risk score is only used to facilitate the ranking of the risk areas. This score is *not* a measure of the organization's compliance effectiveness, nor is it intended to compare, rate, or grade the organization's compliance efforts, controls, or programs against its peers, the market as a whole, or industry best practices. It is also common to map these risk scores visually, often in a grid format, such as the one featured in Figure 10 below. Mapping the scores will enable the organization to quickly view the most critical risk areas (highlighted in red) and will enable the risk management team to deploy a prioritized approach to risk mitigation.

Figure 10: Risk Likelihood-Severity Matrix



- Green: Risks at this level should be monitored but do not necessarily pose any serious threat to the organization at the present.
- Yellow: Organization should take proactive steps to monitor and further evaluate these risk areas and engage mitigation strategies if necessary.
- Red: Immediate action is required to address these risk areas, as the potential for violations or damage to the organization is significant.

J. Step Ten: Finalize Risk Assessment Report and Create Mitigation Action Plan

The last phase of the process is the development of a formal written risk assessment report and the creation of the risk mitigation action plan.

1. Risk Assessment Report

The risk assessment report should be a comprehensive yet easy to understand document reflecting a completed risk assessment process reasonably meeting or exceeding Federal Sentencing Guidelines' risk assessment criteria. The report and supporting documentation must be created, maintained, and delivered in a way that decreases the likelihood of information and the collected data being misconstrued or used out of context. This is important in the event that the organization must later serve as a party, a witness or in a principal in litigation or a government investigation.

Some of the key elements of an effective risk assessment report may include:

- Top Risk Areas: The report should highlight a number of key risk areas.
- Quantification and Ranking of Risk: Each risk area should be weighted for severity and likelihood, then ranked according to the significance of the risk to the organization.
- Supporting Documentation for Risk Quantification: Each risk area and its relative weighting are supported by critical information that should factor into the final report, including existing key aggravating and mitigating factors such as employee knowledge of the risk and the existence or lack of a specific policy or control for the risk.
- Specific Risk-Reducing Steps and Recommendations: Each of the top risk areas should be accompanied by specific actions that the organization can take to reduce its contribution to the quantified risk score and "manage" the risk on an ongoing basis.
- Effectiveness Over Time Measurement: As the organization begins to conduct multiple annual risk assessments, the report should include measurements of the effectiveness of risk management programs by analyzing and tracking the quantification of each major risk area on a year-to-year basis.
- Compliance Program Benchmark: The report should include, if possible, a benchmark of the organization's compliance program and activities compared to its industry peers.

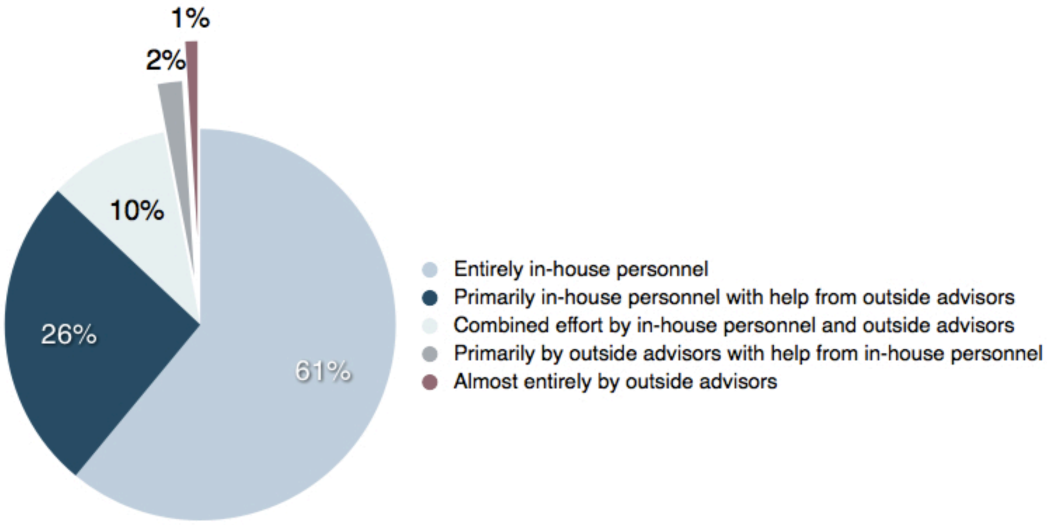
2. Mitigation Action Plan

Once developed, the formal risk assessment report serves as a guide for the creation of an action plan to mitigate the top risks to the organization. This action plan will enable the risk assessment leader to assign specific "risk owners" to lead the process in managing each critical risk area. For each risk, the creation and tracking of clear milestones will help ensure that the process is successfully completed. The action plan itself can take many forms, depending on the organization's desired level of investment. Types of tools used by organizations range from simple documents and Excel-based workbooks to more advanced risk management software packages or web-based applications.

VII. In-House vs. Outsourcing the Risk Assessment

When planning and implementing a risk assessment, every organization faces the decision of whether the assessment should be conducted entirely in-house or if the organization would be better served by hiring external expertise. There are positives and negatives to both approaches and the decision should not be taken lightly. As Figure 11 illustrates, recent survey results show that over half (61 %) of all organizations conduct their risk assessments entirely in-house, while the remainder (39 %) use an outside advisor in the process.

Figure 11: Percentage of Organizations that Conducted Risk Assessments In-House Vs. Using External Advisors or a Combination of Both[18]



A. In-House

Organizations may choose to conduct a risk assessment purely in-house for various reasons, including the size of the organization, budgetary constraints, and concerns over confidentiality. However, there are also limitations to opting to conduct risk assessments internally.

1. Inadequate Process Knowledge

A major concern of internal risk assessment is whether those involved have adequate process knowledge of conducting an effective in-house risk assessment. As demonstrated in this paper, conducting a risk assessment is a methodical engagement with numerous phases requiring substantial coordination and participation of various individuals across the organization. A lack of sufficient process knowledge when conducting these assessments can invite weakened participation and poor coordination across phases, leading to an ultimately ineffective risk assessment.

2. Lack of Templates and Checklists

Vendors who specialize in conducting compliance and ethics risk assessments often leverage existing templates, checklists and other existing tools for a more efficient process. Developing these tools from scratch, as a completely in-house risk assessment might attempt, is inefficient and diversionary.

3. Ineffective Survey Knowledge and/or Interviewing Skills

A significant part of any risk assessment process is the ability to extract the most relevant information from individuals in the organization with expertise in their functional area. To do this, individuals on the risk assessment team must be equipped to ask the right kind of questions. Without this ability, certain risk areas may be substantially understated and the organization may expose itself to future harm.

4. Weak Data Analysis and Interpretation

A good risk assessment process generates a vast amount of data, of which a large portion is qualitative. An inability to accurately translate this collected data into quantifiable terms or properly analyze and interpret it can significantly undermine the results of the risk assessment.

5. Lack of Benchmarks

Conducting the assessment entirely in-house will limit the amount of benchmarking information available compared to leveraging the experience of a qualified vendor.

6. Biased Judgment

Risk assessments require fairly and objectively assessing the full universe of potential risks. An organization must resist any temptation to ignore or de-emphasize risks simply because they may be financially or politically costly to address. To help ensure objectivity, an increasing number of companies are involving domain-expert external advisors in the assessment.

B. Hire Outside Advisors

Organizations may also choose to hire the expertise of outside advisors or experts to help them conduct the organizational risk assessment.

1. Who Are They?

Depending on the level of knowledge or expertise required, an organization can seek to hire the resources of:

- Outside lawyers or law firm.
- Audit firms.

- Other compliance experts, consultants, etc.

2. Why it is a Good Idea?

There are several reasons, not always readily apparent, why utilizing the advice, counsel or services of an external advisor is a good idea. A few of these reasons are detailed below.

a. Document/Information Security

One of the benefits of using an outside advisor is the ability to keep sensitive or potentially damaging information off company premises. By utilizing an independent third party, much of the information generated can be stored, maintained, or held by the third party. This is very important, as the various documents created may detail potential compliance problems of varying levels of severity. By keeping the information with a third party, the organization can better protect itself from private litigants and/or regulatory bodies obtaining this information and using it as evidence of pre-existing knowledge of compliance failures.

b. Analytical and/or Statistical Expertise

An effective risk assessment requires a high level of analytical and statistical expertise. Although some organizations may be adept and experienced at conducting risk assessments, relying on the available skills and experience of outside consultants, who have current knowledge of the intricacies and frequent changes in the risk management field, is often a wise choice.

c. Non-Biased

When conducting a risk assessment internally, a natural bias will always exist. Individuals who are too close to the business operations will have a tendency to misinterpret information and might overestimate or underestimate the extent of a potential risk to the organization. This bias introduces questions regarding the credibility of the risk assessment itself. As such, hiring an independent outside observer to help manage part or all of the risk assessment will help prevent the effects of organizational bias.

VIII. Glossary

Below are summary definitions of some of the terms used in this InfoPAK^{SM}.

A. Enterprise Impact

A product of risk severity and likelihood of occurrence, Enterprise Impact is the significance or effect (either positive or negative) that a unique risk or risks can have on an organization.

B. External Aggravating Factors

The factors (political, legal, environmental, socioeconomic, etc.) outside of the actual organization, which play a role in subjecting the organization to heightened risk.

C. Internal Aggravating Factors

The factors specific to an organization's unique circumstances or operation. Such factors can be identified through a number of methods, including, but not limited to, interviews, assessments/surveys, examinations of available policies and procedures, financial reporting, etc.

D. Internal Mitigating Factors

These pertain to specific elements unique to the organization that can provide a reduction effect to identified risk areas relevant to the organization.

E. Occurrence Likelihood

The reasonable likelihood of a risk event occurring for a typical or average company in a given industry.

F. Risk Severity

The maximum potential economic outcome of violation or misconduct for a typical company in a given industry, measured in terms of total enterprise impact.

G. Risk Area Weighting

Practice of assigning unique values or ratings to areas of risk, where the specific weights are quantified by both impact and likelihood of occurrence.

H. Risk Assessment Team

Collection of individuals or employees of an organization tasked with the responsibility of researching and evaluating the overall environment of risk in the organization, as well as recommending future action to manage identified risk areas.

I. Risk Universe

This term pertains to a catalog or inventory of identified risk areas relevant to the subject organization.

J. Sarbanes-Oxley § 404

Pertains to the information detailed in Section 404 of the Sarbanes-Oxley Act of 2002 ("SOX 404"). This section outlines the requirements for a publicly traded organization to present a Management Assessment of Internal Controls when issuing an annual report.

K. PCAOB Auditing Standard #5

Pertains to AS#5 that recently replaced AS#2. Approved by the SEC in July 2007, AS#2 is aimed at improving the accuracy of financial reports while reducing unnecessary costs, especially for smaller companies. The standard allows management to rely on assessment of internal controls by other independent managers when certifying to the effectiveness of internal controls to meet SOX 404 requirements.

IX. About the Author

Corpedia Corporation, founded in 1998, offers a wide variety of innovative and user-friendly compliance and ethics solutions. Developed and implemented by a team of experts with years of experience and industry insight, our compliance risk assessment solutions identify, quantify and provide actionable plans for mitigating and preventing compliance breakdowns. Our e-learning programs bolster these assessments by familiarizing employees with all facets of regulations affecting their company and offering the most measurable outcomes for their compliance and ethics initiatives. With over 600 customers in more than 150 countries, including Wal-Mart, Time Warner, OfficeMax, Dun & Bradstreet and PepsiCo, Corpedia delivers the right compliance and ethics solutions to the right people at the right time-every time.

X. Additional Resources

A. ACC Docket Articles

Diana Jimenez, “Performing a Privacy Risk Assessment,” *ACC Docket* 27, no. 9 (Nov. 2009), *available at* http://www.acc.com/legalresources/resource.cfm?show=721374.

Arleigh V. Closser and David P. Anderson, “Risk Management: Should Corporate Counsel Lead the Charge?” *ACC Docket* 26, no. 9 (Nov. 2008): 56-65, *available at* http://www.acc.com/legalresources/resource.cfm?show=86548.

Bao Q. Tran and Jonathan P. Tomes, “Risk Analysis: Your Key to Compliance,” *ACC Docket* 21, no. 10 (Nov. 2003): 38-54, *available at* http://www.acc.com/legalresources/resource.cfm?show=17069.

B. ACC Annual Meeting Material

John Beccia III ET AL., “Challenges Faced When Establishing an Enterprise-Wide Compliance Risk Management Program,” ACC 2007 Annual Meeting, Session 208, *available at* http://www.acc.com/legalresources/resource.cfm?show=19957.

C. ACC InfoPAKs^{SM}

“Compliance Training and E-Learning Programs: Leading Practices in Designing, Implementing, and Supporting Risk Assessment and Communication Strategies,” ACC InfoPAK (July 2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=19710.

“Effective Compliance and Ethics for the Small Law Department - Doing More With Less,” ACC InfoPAK (July 2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=19635.

“Corporate Compliance,” ACC InfoPAK (Aug. 2009), *available at* http://www.acc.com/legalresources/resource.cfm?show=19684.

D. ACC Webcasts

“Corporate Compliance Risk Assessments – Methodologies and Benchmarks from Leading Corporations,” ACC Webcast (May 11, 2006), *available at* http://www.acc.com/legalresources/resource.cfm?show=16389.

E. Other Resources

“Benchmark Survey of In-House Counsel Roles and Attitudes in Relation to Compliance, Ethics and Corporate Social Responsibility Activities,” ACC/Corpedia Survey (2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=806873.

“Checklist on Basic Compliance Risks,” ACC Quick Reference (June 2009), *available at* http://www.acc.com/legalresources/resource.cfm?show=800383.

“How To Assess Legal Risk Management Practices,” ACC Value Challenge Tool Kit Resource (Oct. 2008), *available at* http://www.acc.com/legalresources/resource.cfm?show=38926.

“How to Focus Internal Communications About Legal Risk,” ACC Value Challenge Tool Kit Resource (Oct. 2008), *available at* http://www.acc.com/legalresources/resource.cf m?show=39706.

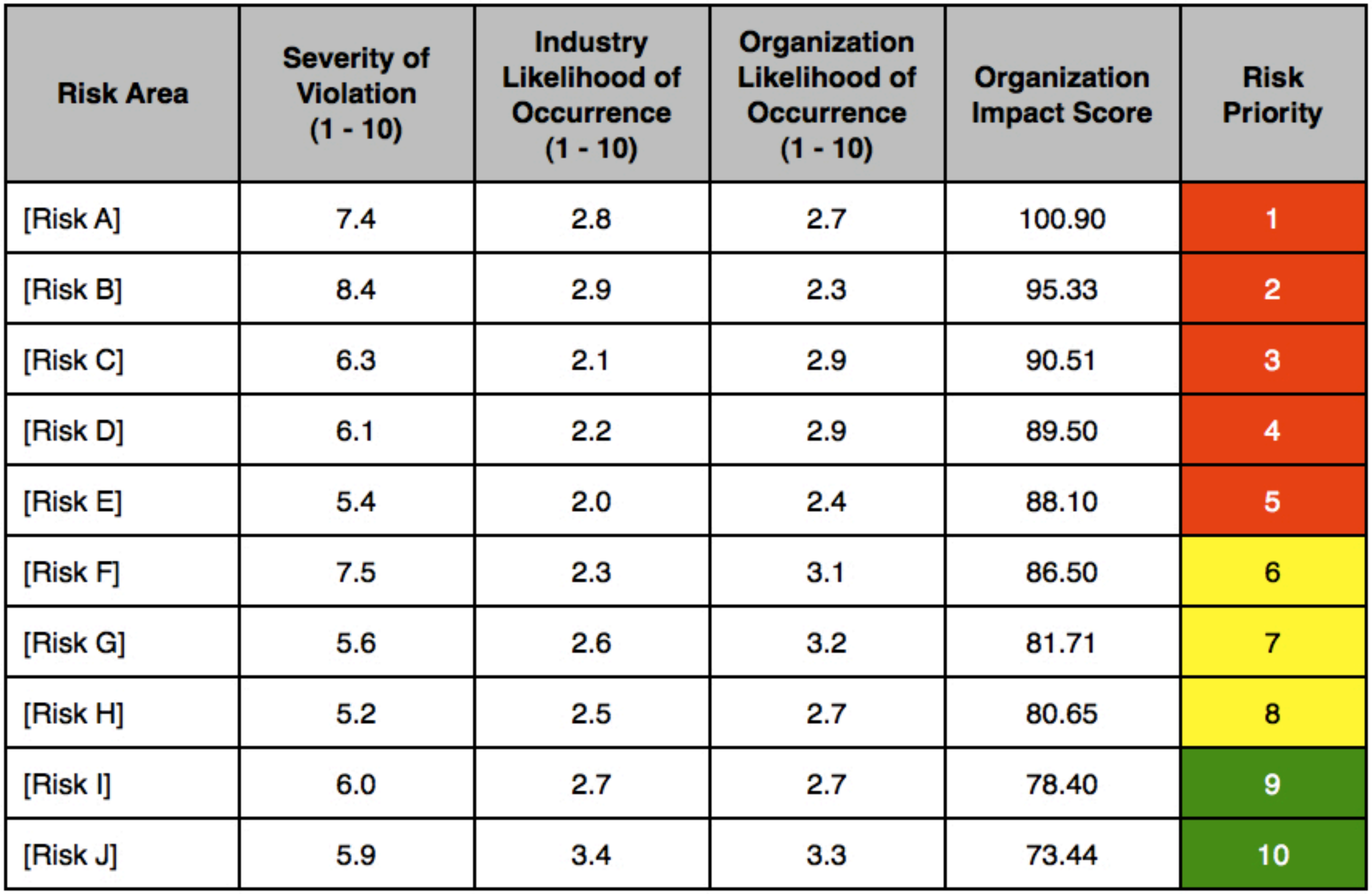
"How to Identify Business Processes for Legal Risks," ACC Value Challenge Tool Kit Resource (Sept. 2008), *available at* http://www.acc.com/legalresources/resource.cfm?show=39895.

"How To Identify Legal Risks in Business Processes," ACC Value Challenge Tool Kit Resource (Sept. 2008), *available at* http://www.acc.com/legalresources/resource.cfm?show=40045.

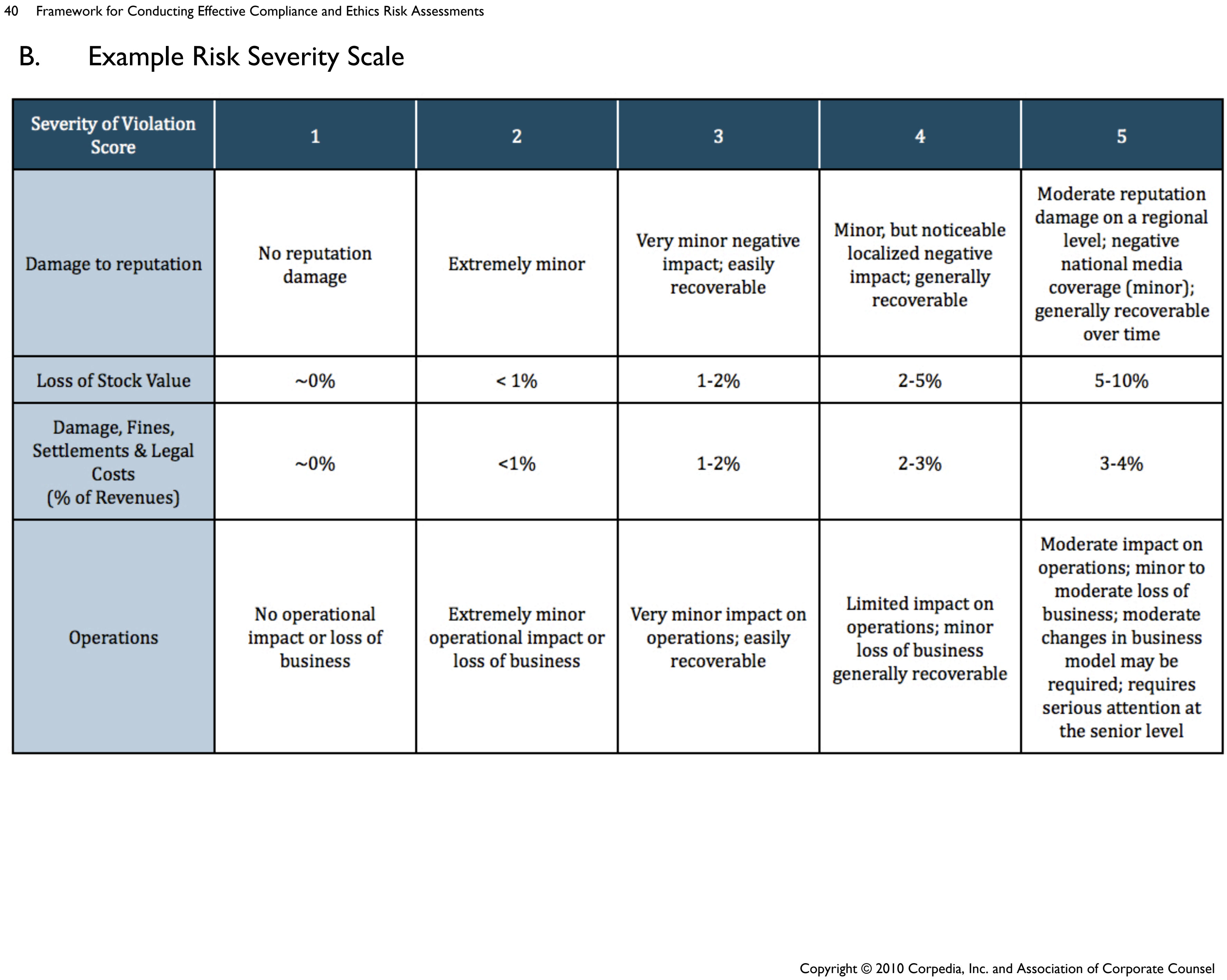
"Strategic Issues in Intellectual Property Risk Management," ACC CLO Think Tank Series Briefing Material (June 1, 2007), *available at* http://www.acc.com/community/clo/thinktanks/Strategic-Issues-in-Intellectual-Property-Risk-Management.cfm.

XI. Sample Forms

A. Risk Universe Chart



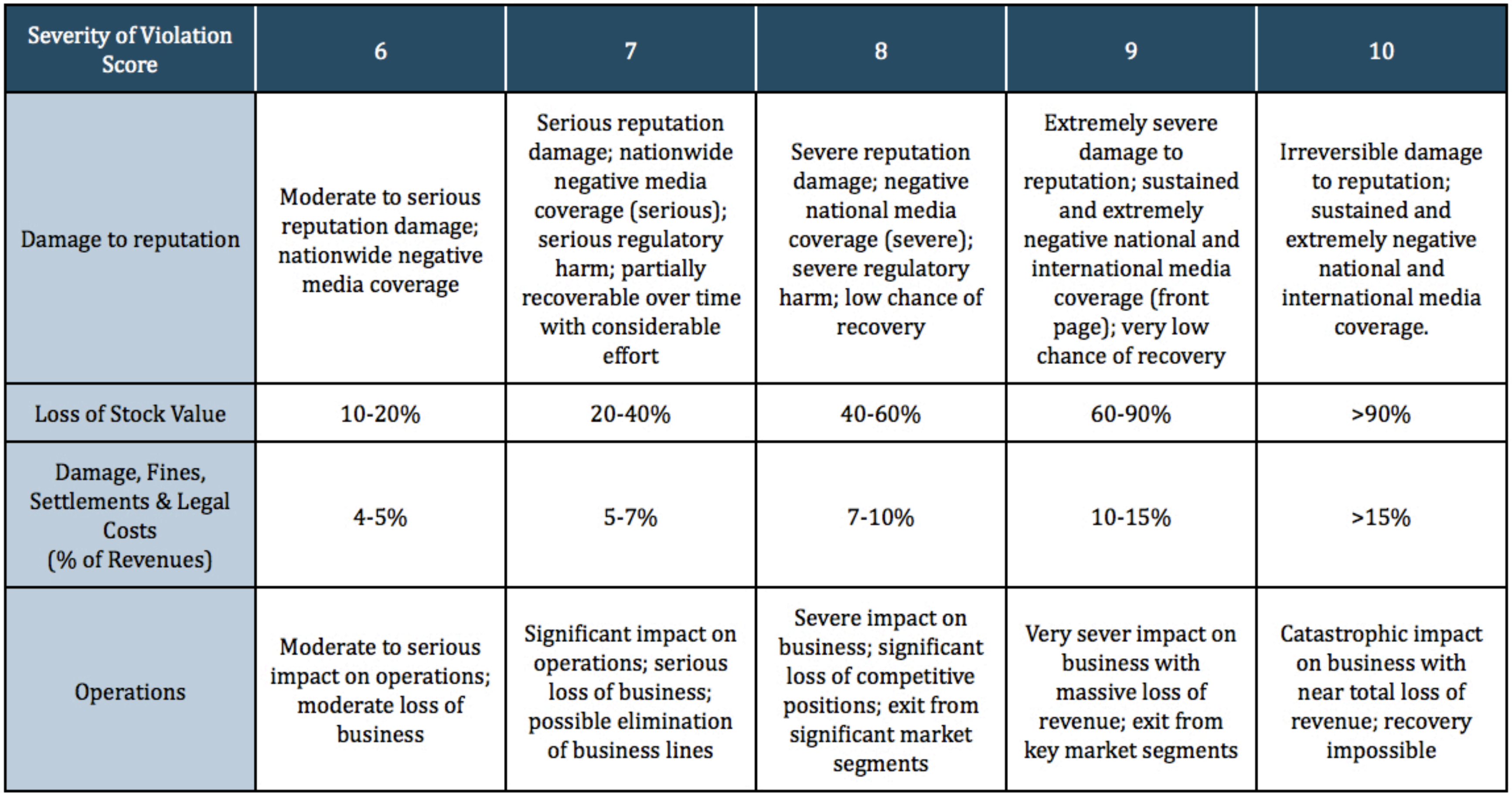
Risk Area	Severity of Violation (1 - 10)	Industry Likelihood of Occurrence (1 - 10)	Organization Likelihood of Occurrence (1 - 10)	Organization Impact Score	Risk Priority
[Risk A]	7.4	2.8	2.7	100.90	1
[Risk B]	8.4	2.9	2.3	95.33	2
[Risk C]	6.3	2.1	2.9	90.51	3
[Risk D]	6.1	2.2	2.9	89.50	4
[Risk E]	5.4	2.0	2.4	88.10	5
[Risk F]	7.5	2.3	3.1	86.50	6
[Risk G]	5.6	2.6	3.2	81.71	7
[Risk H]	5.2	2.5	2.7	80.65	8
[Risk I]	6.0	2.7	2.7	78.40	9
[Risk J]	5.9	3.4	3.3	73.44	10



B. Example Risk Severity Scale

Severity of Violation Score	1	2	3	4	5
Damage to reputation	No reputation damage	Extremely minor	Very minor negative impact; easily recoverable	Minor, but noticeable localized negative impact; generally recoverable	Moderate reputation damage on a regional level; negative national media coverage (minor); generally recoverable over time
Loss of Stock Value	~0%	< 1%	1-2%	2-5%	5-10%
Damage, Fines, Settlements & Legal Costs (% of Revenues)	~0%	<1%	1-2%	2-3%	3-4%
Operations	No operational impact or loss of business	Extremely minor operational impact or loss of business	Very minor impact on operations; easily recoverable	Limited impact on operations; minor loss of business generally recoverable	Moderate impact on operations; minor to moderate loss of business; moderate changes in business model may be required; requires serious attention at the senior level

C. Example Risk Severity Scale (Continued)



Severity of Violation Score	6	7	8	9	10
Damage to reputation	Moderate to serious reputation damage; nationwide negative media coverage	Serious reputation damage; nationwide negative media coverage (serious); serious regulatory harm; partially recoverable over time with considerable effort	Severe reputation damage; negative national media coverage (severe); severe regulatory harm; low chance of recovery	Extremely severe damage to reputation; sustained and extremely negative national and international media coverage (front page); very low chance of recovery	Irreversible damage to reputation; sustained and extremely negative national and international media coverage.
Loss of Stock Value	10-20%	20-40%	40-60%	60-90%	>90%
Damage, Fines, Settlements & Legal Costs (% of Revenues)	4-5%	5-7%	7-10%	10-15%	>15%
Operations	Moderate to serious impact on operations; moderate loss of business	Significant impact on operations; serious loss of business; possible elimination of business lines	Severe impact on business; significant loss of competitive positions; exit from significant market segments	Very sever impact on business with massive loss of revenue; exit from key market segments	Catastrophic impact on business with near total loss of revenue; recovery impossible

XII. Endnotes

[1] *See generally* PROJECT MANAGEMENT INSTITUTE, A GUIDE TO THE PROJECT MANAGEMENT BODY OF KNOWLEDGE (PMBOK® GUIDE) (4th ed. 2008), *available for purchase at* http://www.pmi.org/Resources/Pages/Library-of-PMI-Global-Standards-projects.aspx.

[2] U.S. SENTENCING GUIDELINES MANUAL § 8B2.1(c) (2009).

[3] "Benchmark Survey of In-House Counsel Roles and Attitudes in Relation to Compliance, Ethics and Corporate Social Responsibility Activities," ACC/Corpedia Survey (2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=806873.

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *See id.*

[8] *See* Tool Nine, "Effective Compliance and Ethics Programs for the Small Law Department," ACC InfoPAK (Aug. 2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=19635.

[9] U.S. SENTENCING GUIDELINES MANUAL § 8B2.1 cmt. n.6 (2009).

[10] For more information on ECERA™, visit http://welcome.corpedia.com/advisory-services/risk-assessment-ecera.

[11] OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB CIRC. A-133, AUDITS OF STATES, LOCAL GOVERNMENTS AND NON-PROFIT ORGANIZATIONS (rev. 2007), *available at* http://www.whitehouse.gov/omb/asset.aspx?AssetId=2434.

[12] Sarbanes-Oxley Act of 2002 § 404, 15 U.S.C. § 4262 (2006).

[13] For more on COSO methodology, visit http://www.coso.org/GuidanceonMonitoring.htm.

[14] *Id.*

[15] PUB. CO. ACCOUNTING OVERSIGHT BD., AUDITING STANDARD NO. 5, INTERNAL CONTROL OVER FINANCIAL REPORTING (2007), *available at* http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx.

[16] "Benchmark Survey," *supra* note 3.

[17] Organizations commonly rely on Corpedia's ECERA™ database for such a benchmarking activity, as it contains specific, critical risk severity metric data for over fifty unique industries, collected as a result of in-depth research of over 1,000 U.S. and international corporations.

[18] "Benchmark Survey," *supra* note 3.