

# The **LEXIS PRACTICE ADVISOR** Journal™

Practical guidance backed by experts from Lexis Practice Advisor®

## **NAVIGATING COMPLIANCE CONCERNS**

**In-House Counsel's Role in  
Cybersecurity and Data Protection**

**Top Ten Practice Tips:  
Public Company Reporting**



 LexisNexis®

**CORPORATE COUNSEL**

**Special Edition 2017**





LexisNexis®

Lexis® for Microsoft® Office

# DELIVER BULLETPROOF CONTRACTS

TRUSTED PRACTICAL GUIDANCE AND  
PRECISE PROOFREADING TOOLS  
RIGHT WITHIN YOUR DOCUMENT

*Start your free trial today*

**LEXISNEXIS.COM/BULLETPROOF**  
**OR CALL 888.285.3947**

**21**

LEGAL DRAFTING  
TOOLS



INTEGRATED INTO  
WORD & OUTLOOK®

**650+**

ATTORNEY  
AUTHORS

**14**

PRACTICE AREAS  
WITH EXPERT GUIDANCE

# Contents

CORPORATE COUNSEL SPECIAL EDITION 2017

## PRACTICE NEWS

### 4 CURRENT UPDATES AND LEGAL DEVELOPMENTS

*Corporate Counsel, Intellectual Property, Finance, Labor & Employment, Employee Benefits & Executive Compensation*

## GC ADVISORY

### 12 TOP TEN PRACTICE TIPS: PUBLIC COMPANY REPORTING

*Capital Markets & Corporate Governance*

## PRACTICE POINTERS

### 16 NAVIGATING COMPLIANCE CONCERNS

*Commercial Transactions*

### 28 CONDUCTING A RISK ASSESSMENT

*General Practice*

### 32 CHECKLIST-15 SAMPLE QUESTIONS WHEN PERFORMING A RISK ASSESSMENT

*General Practice*

## PRACTICE TRENDS

### 34 KEY ISSUES EMPLOYERS SHOULD CONSIDER WHEN INTEGRATING ROBOTICS AND AUTOMATION IN THE WORKPLACE

*Labor & Employment*

### 40 IN-HOUSE COUNSEL'S ROLE IN CYBERSECURITY AND DATA PROTECTION

*IP & Technology*

### 47 WHAT COMPANIES NEED TO KNOW ABOUT PROTECTING CONFIDENTIAL INFORMATION UNDER THE NEW ACC GUIDELINES

*IP & Technology*

## PRACTICE NOTES

### 52 ADDRESSING RETIREMENT PLAN INVESTMENT COMMITTEE ISSUES

*Employee Benefits & Executive Compensation*

### 62 ATTORNEY-CLIENT PRIVILEGE CONSIDERATIONS FOR PRIVATE EQUITY FIRM COUNSEL

*Corporate and M&A*

## IN-HOUSE INSIGHTS

### 67 IN-HOUSE COUNSEL ETHICS: FEE SHARING IMPLICATIONS

*Corporate Counsel*

## PRACTICE PROJECTIONS

### 70 MARKET TRENDS: RESPONDING TO NEGATIVE VOTING RECOMMENDATIONS BY FILING ADDITIONAL PROXY SOLICITING MATERIALS

*Capital Markets & Corporate Governance*





# The LEXIS PRACTICE ADVISOR Journal™

SPECIAL EDITION 2017 (Volume 2, Issue 3 - Corporate Counsel)

EDITOR-IN-CHIEF  
**Eric Bourget**

VP, LEXIS PRACTICE ADVISOR  
AND ANALYTICAL  
VP, ANALYTICAL LAW  
& LEGAL NEWS  
MANAGING EDITOR  
DESIGNER  
MARKETING

**Rachel Travers**  
**Aileen Stirling**  
**Lori Sieron**  
**Jennifer Shadbolt**  
**Sarah Patrick**  
**Karen Victoriano**  
**Jake Miller**

## CONTRIBUTING EDITORS

Finance, Financial  
Restructuring & Bankruptcy  
Banking Law  
Capital Markets  
Commercial Transactions  
Corporate Counsel  
Employee Benefits  
& Executive Compensation  
Intellectual Property & Technology  
Labor & Employment  
Mergers & Acquisitions  
Oil & Gas, Jurisdictional  
Real Estate  
Tax

**Robyn Schneider**  
**Matthew Burke**  
**Burcin Eren**  
**Anna Haliotis**  
**Carrie Wright**  
**Bradley Benedict**  
**Jessica McKinney**  
**Elias Kahn**  
**Dana Hamada**  
**Cameron Kinvig**  
**Lesley Vars**  
**Jessica Kerner**

ASSOCIATE EDITORS

**Maureen McGuire**  
**Mary McMahon**  
**Erin Webreck**  
**Ted Zwyer**

PRINTED BY

**Cenveo Publisher Services**  
**3575 Hempland Road**  
**Lancaster, PA 17601**



## EDITORIAL ADVISORY BOARD

Distinguished Editorial Advisory Board Members for The Lexis Practice Advisor Journal are expert practitioners with extensive background in the transactional practice areas included in Lexis Practice Advisor®. Many are attorney authors who regularly provide their expertise to Lexis Practice Advisor online and have agreed to offer insight and guidance for The Lexis Practice Advisor Journal. Their collective knowledge comes together to keep you informed of current legal developments and ahead of the game when facing emerging issues impacting transactional practice.

**Andrew Bettwy, Partner**  
Proskauer Rose LLP  
Finance, Corporate

**Joseph M. Marger, Partner**  
Reed Smith LLP  
Real Estate

**Julie M. Capell, Partner**  
Davis Wright Tremaine LLP  
Labor & Employment

**Alexandra Margolis, Partner**  
Nixon Peabody LLP  
Banking & Finance

**Candice Choh, Partner**  
Gibson Dunn & Crutcher LLP  
Corporate Transactions,  
Mergers & Acquisitions

**Matthew Merkle, Partner**  
Kirkland & Ellis International LLP  
Capital Markets

**S. H. Spencer Compton, VP,  
Special Counsel**  
First American Title Insurance Co.  
Real Estate

**Timothy Murray, Partner**  
Murray, Hogue & Lannis  
Business Transactions

**Linda L. Curtis, Partner**  
Gibson, Dunn & Crutcher LLP  
Global Finance

**Michael R. Overly, Partner**  
Foley & Lardner  
Intellectual Property, Technology

**Tyler B. Dempsey, Partner**  
Troutman Sanders LLP  
Mergers & Acquisitions, Joint  
Ventures

**Leah S. Robinson, Partner**  
Mayer Brown LLP  
State and Local Tax

**James G. Gatto, Partner**  
Sheppard, Mullin, Richter &  
Hampton LLP  
Intellectual Property, Technology

**Scott L. Semer, Partner**  
Torys LLP  
Tax, Mergers and Acquisitions

**Ira Herman, Partner**  
Blank Rome LLP  
Insolvency and Commercial Litigation

**Claudia K. Simon, Partner**  
Schulte Roth & Zabel  
Corporate, Mergers & Acquisitions

**Ethan Horwitz, Partner**  
Carlton Fields Jordan Burt  
Intellectual Property

**Lawrence Weinstein,  
Corporate Counsel**  
The Children's Place Inc.

**Glen Lim, Partner**  
Katten Muchin Rosenman LLP  
Commercial Finance

**Kristin C. Wigness, First V.P.  
& Associate General Counsel**  
Israel Discount Bank of New York  
Lending, Debt Restructuring,  
Insolvency

**Patrick J. Yingling, Partner**  
King & Spalding  
Global Finance

The Lexis Practice Advisor Journal (Pub No. 02380; ISBN: 978-1-63284-895-6) is a complimentary publication published quarterly for Lexis Practice Advisor® subscribers by LexisNexis, 230 Park Avenue, 7th Floor, New York, NY 10169. Email: [lexispracticeadvisorjournal@lexisnexis.com](mailto:lexispracticeadvisorjournal@lexisnexis.com) | Website: [www.lexisnexis.com/lexispracticeadvisorjournal](http://www.lexisnexis.com/lexispracticeadvisorjournal)

This publication may not be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form, in whole or in part, without prior written consent of LexisNexis. Reproduction in any form by anyone of the material contained herein without the permission of LexisNexis is prohibited. Permission requests should be sent to: [permissions@lexisnexis.com](mailto:permissions@lexisnexis.com).

All information provided in this document is general in nature and is provided for educational purposes only. It may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual cases. It should not be construed as legal advice. For legal advice applicable to the facts of your particular situation, you should obtain the services of a qualified attorney licensed to practice in your state.

The publisher, its editors and contributors accept no responsibility or liability for any claims, losses or damages that might result from use of information contained in this publication. The views expressed in this publication by any contributor are not necessarily those of the publisher.

Send address changes to: The Lexis Practice Advisor Journal, 230 Park Avenue, 7th Floor, New York, NY 10169. Periodical Postage Paid at New York, New York, and additional mailing offices.

LexisNexis, the Knowledge Burst logo and Lexis Practice Advisor are registered trademarks and Lexis Practice Advisor Journal is a trademark of Reed Elsevier Properties Inc., used under license. Other products and services may be trademarks or registered trademarks of their respective companies.

Copyright 2017 LexisNexis. All rights reserved. No copyright is claimed as to any part of the original work prepared by a government officer or employee as part of that person's official duties.

Cover photo courtesy Csaba Peterdi / Shutterstock.com. Additional images used under license from Shutterstock.com.



**Rachel Travers, VP of Lexis Practice Advisor and Analytical**

#### WELCOME TO THE CORPORATE COUNSEL

Special Edition of The Lexis Practice Advisor Journal, and thank you to the fantastic Practice Advisor Journal team for the invitation to prepare this introduction.

Lexis Practice Advisor is such a special, important piece of what we do here at LexisNexis both here in the United States and across the globe. In today's fast-paced legal environment, we recognize that you're increasingly burdened with heavier workloads, quicker turnarounds and higher client expectations, while also asked to deliver more noticeable positive results. Lexis Practice Advisor provides a great starting

point for tackling these growing demands. By empowering you to work better, faster and smarter, practical guidance truly delivers a tangible advantage—which is why we continue to invest globally in improving and adding to the content, technology and functionality available to you.

We've recently announced several updates to Lexis Practice Advisor, which we feel truly deliver an enhanced, intuitive user experience and provide easier and faster access to vital information in addition to providing you with more content. First, we launched a newly redesigned Lexis Practice Advisor interface, which includes a more streamlined look and additional navigation options, designed to improve your workflow and output. We also launched two new modules, Employee Benefits & Executive Compensation and Pennsylvania Practice, bringing specialized content, advice, forms, checklists and more to these specific areas. Finally, we integrated applications from the Intelligize service into various modules of Lexis Practice Advisor, granting module-specific users access to deal information on M&A transactions and securities offerings as well as thousands of precedent agreements, SEC filings and other deal-related documents.

These new enhancements and launches were built with you in mind. Our goal has been to create a product that is as intuitive and user-friendly as possible, while providing attorneys with the high-value, easy-to-digest content needed to complete any legal task quickly and efficiently. With these enhancements, we're continuing to do just that.

In this special edition of The Lexis Practice Advisor Journal, we're specifically targeting content relevant to corporate, in-house and general counsel attorneys, with an emphasis on data security, risk assessment and compliance. Within this issue, you'll find a series of articles around these topics, including but not limited to: tips about how to align internal and external resources to best manage the data security procedures a company must implement in order to comply with regulations and protect data; a practical guide on creating, developing and implementing a compliance program that can be used globally, regardless of industry or the size of your company; and an article on completing a well-devised risk assessment to best identify specific vulnerabilities and help business leaders effectively manage and mitigate the organization's legal and regulatory risk.

## Our mission

*The Lexis Practice Advisor Journal™ is designed to help attorneys start on point. This supplement to our online practical guidance resource, Lexis Practice Advisor®, brings you a sophisticated collection of practice insights, trends, and forward-thinking articles. Grounded in the real-world experience of our 650+ seasoned attorney authors, the Lexis Practice Advisor Journal offers fresh, contemporary perspectives and compelling insights on matters impacting your practice.*



## SUPREME COURT TO RULE ON VALIDITY OF CLASS WAIVERS IN EMPLOYMENT CONTEXT

**THE U.S. SUPREME COURT IS** expected to decide this term whether the collective-bargaining provisions of the [National Labor Relations Act](#) (NLRA) prohibit enforcement of agreements requiring employees to arbitrate claims against employers on an individual, rather than collective or class action, basis.

The high court in June granted three petitions for writ of certiorari to resolve a conflict among the federal circuit courts on the question. At issue is the National Labor Relations Board's (NLRB) position, set forth in [In re Horton, 357 NLRB No. 184 \(January 2012\)](#), that the NLRA guarantees the right of employees to act collectively to address employment claims and that requiring employees to waive that right is a violation of the statute.

The U.S. Court of Appeals for the Seventh Circuit and the U.S. Court of Appeals for the Ninth Circuit have agreed with the NLRB's stance, while the U.S. Court of Appeals for the Fifth Circuit has rejected the NLRB's position.

The Department of Justice (DOJ) has weighed in on the issue, contending in an amicus curiae brief that the NLRB's interpretation runs afoul of the presumption contained in the [Federal Arbitration Act](#) (FAA) that arbitration agreements are valid unless the FAA's mandate has been overridden by congressional action or enforcement would vitiate a substantial federal right. "Neither of those justifications for non-enforcement is applicable here," the DOJ said.

Dozens of amicus curiae briefs have been filed on both sides of the issue, with unions

and employee groups supporting the NLRB's position, and business groups, including the U.S. Chamber of Commerce, weighing in on the side of employers.

The three cases, which were consolidated for oral argument before the Supreme Court, are [Ernst & Young LLP v. Stephen Morris, No. 16-300](#); [NLRB v. Murphy Oil USA Inc., No. 16-307](#); and [Epic Systems Corp. v. Lewis, No. 16-285](#).

A decision is expected by the end of the high court's current term.

*-Lexis Practice Advisor Staff*



**RESEARCH PATH:** [Labor and Employment > Employment Contracts > Waivers and Releases > Articles](#)

---

# OMB STAYS EFFECTIVENESS OF REVISIONS TO EEOC FORM PENDING MORE INFORMATION

---

**THE FEDERAL OFFICE OF** Management and Budget (OMB) has directed the Equal Employment Opportunity Commission (EEOC) to stay the effectiveness of certain revisions to the EEOC's EEO-1 form. The affected revisions, issued on Sept. 29, 2016, relate to new requests for data on wages and hours worked from employers with 100 or more employees and federal contractors with 50 or more employees.

The OMB noted that since the revised EEO-1 form was approved, the EEOC released data file specifications for employers to use in submitting the form. However, the specifications were not contained in the original Federal Register notices seeking public comment on the revisions and were

not outlined in the supporting statement for the collection of the information, the OMB said. "As a result," the OMB said, "the public did not receive an opportunity to provide comment on the method of data submission to EEOC."

In addition, the OMB stated that the burden estimates submitted by the EEOC did not account for the use of the data file specifications, "which may have changed the initial burden estimate."

The stay is necessary, the OMB said, because of concerns "that some aspects of the revised collection of information lack practical utility, are unnecessarily burdensome, and do not adequately address privacy and confidential issues."

The OMB ordered the EEOC to submit a new information collection package for its review and to publish a notice in the Federal Register announcing the immediate stay of the wage and hours reporting requirements in the revised form. Employers may continue to use the previously approved EEO-1 form to meet their reporting obligations for FY 2017.

*-Adapted from Benders Labor & Employment Bulletin, Volume 17, Issue 9*



**RESEARCH PATH:** [Labor &](#)

[Employment > Employment](#)

[Policies > Equal Employment Opportunity](#)

[> Articles](#)





# EMPLOYEE CAN SUE FOR MEDICAL MARIJUANA-RELATED FIRING, MASSACHUSETTS COURT RULES

## AN EMPLOYEE WHO WAS TERMINATED FOR TESTING

positive for the lawful use of medical marijuana can bring an action for handicap discrimination under state law, the Massachusetts Supreme Judicial Court has held.

Massachusetts law provides for lawful use of medical marijuana for “qualified patients” under an initiative petition passed by voters in 2012 ([An Act for the Humanitarian Medical Use of Marijuana](#)).

The court said that Cristina Barbuto meets the state anti-discrimination statute’s ([ALM GL ch. 151B, § 1\(16\)](#)) definition of “qualified handicapped person” by virtue of her diagnosis of Crohn’s disease, for which her physician prescribed medical marijuana.

Barbuto was hired by Advantage Sales and Marketing (ASM) in late summer 2014. She told her supervisor that a mandatory drug test would prove positive for marijuana, but she was assured that because her use was lawful under state law, the positive result would not be an issue. After the test came back positive, she was terminated for violation of the company’s drug policy. ASM acknowledged that Barbuto was protected by state law, but it cited federal law against marijuana use as the basis for its decision.

Barbuto filed suit in state court, asserting causes of action for handicap discrimination, invasion of privacy, and violation of the medical marijuana statute. ASM moved to dismiss the suit; the trial court dismissed all but the invasion of privacy claim. The Supreme Judicial Court granted Barbuto’s petition for direct appeal.

Reversing with respect to the handicap discrimination claim, the state high court held that Barbuto’s condition falls within the protection of the anti-discrimination statute and that because the

use of medical marijuana is legal under Massachusetts law, ASM was required to provide a reasonable accommodation for Barbuto’s illness. However, the court said that its ruling does not necessarily mean a victory for Barbuto. [Barbuto v. Advantage Sales and Marketing, LLC, 477 Mass. 456 \(Mass. 2017\)](#).

“Our conclusion that an employee’s use of medical marijuana under these circumstances is not facially unreasonable as an accommodation for her handicap means that the dismissal of the counts alleging handicap discrimination must be reversed,” the court said. “But it does not necessarily mean that the employee will prevail in proving handicap discrimination. The defendant at summary judgment or trial may offer evidence to meet their burden to show that the plaintiff’s use of medical marijuana is not a reasonable accommodation because it would impose an undue hardship on the defendant’s business.”

The court affirmed the dismissal of Barbuto’s claim under the medical marijuana statute, however, finding that the statute did not create a private cause of action for employees.

The court noted that the vast majority of states, along with the District of Columbia and Puerto Rico, have allowed limited possession of marijuana for medical treatment, making the issue of use of medical marijuana an issue that will continue to arise in the workplace.

-Lexis Practice Advisor Staff



RESEARCH PATH: [Labor and Employment](#) > [Employment Policies](#) > [Safety and Health](#) > [Articles](#)







## OSHA LAUNCHES E-FILING FOR MANDATORY INJURY AND ILLNESS REPORTS

**THE OCCUPATIONAL SAFETY AND** Health Administration's (OSHA) electronic portal, the Injury Tracking Application (ITA), is now live for employers to file reports of workplace illnesses and injuries. OSHA's electronic record-keeping rule, which applies to companies with 250 employees or more, requires employers to submit electronically the OSHA Form 300 (Log of Work-Related Injuries and Illnesses), OSHA Form 300A (Summary of Work-Related Injuries and Illnesses), and OSHA Form 301

(Injury and Illness Incident Report). These forms are available at <https://www.osha.gov/recordkeeping/RKforms.html>.

Employers with 20–249 employees in industries with historically high rates of occupational injuries and illnesses must electronically submit the information from the OSHA Form 300A. These industries include construction, utilities, equipment rentals, and commercial machinery repair and maintenance, among others. Employers

have three options for submitting their 300A data electronically: manually entering data into a web form, uploading a CSV file, or transmitting data electronically with an application programming interface.

*-Benders Labor & Employment Bulletin, Volume 17, Issue 9*



**RESEARCH PATH:** [Labor & Employment > Employment Policies > Safety & Health > Articles](#)

[www.lexispracticeadvisor.com](http://www.lexispracticeadvisor.com)



---

# DEPARTMENT OF LABOR PROPOSES EXTENDED TRANSITION FOR FIDUCIARY RULE EXEMPTION

---

**THE U.S. DEPARTMENT OF LABOR (DOL) HAS PROPOSED** an 18-month expansion of the transition period leading up to effectiveness of the Best Interest Contract (BIC) and Principal Transactions exemptions to the DOL's Fiduciary Rule. The proposal calls for extending the end of the period from January 1, 2018, to July 1, 2019.

The Fiduciary Rule refers to the designation of brokers, investment advisors, insurance agents, and other financial professionals as fiduciaries with respect to plans governed by the Employee Retirement Income Security Act (ERISA).

The proposal comes after a Request for Information published by the DOL in July seeking public input on new exemptions or changes to the rule and exemptions, as well as the advisability of extending the transition period.

At the same time, the DOL announced an enforcement policy related to the arbitration provision contained in the two exemptions.

The arbitration provision makes the exemptions unavailable if a financial institution's contract with a retirement investor includes a waiver or qualification of the retirement investor's right to participate in a class action or other court action. The DOL's policy comes after Acting U.S. Solicitor General Jeffrey B. Wall indicated, in an amicus brief filed in *NLRB v. Murphy Oil USA Inc.* (No. 16-307, U.S. Sup.) currently pending before the U.S. Supreme Court, the federal government's intention to refrain from defending the provisions as applied to arbitration agreements preventing investors from participating in class-action litigation.

*-Lexis Practice Advisor Staff*



**RESEARCH PATH:** [Employee Benefits & Executive](#)

[Compensation > Retirement Plans > ERISA and Fiduciary](#)

[Compliance > Articles](#)



# DELAWARE JUDGE FINDS PERMANENT PRESENCE NECESSARY FOR PATENT INFRINGEMENT SUIT VENUE

**IN TWO RULINGS ISSUED THE SAME DAY, A FEDERAL judge in Delaware has interpreted the patent venue statute's "regular and established place of business" language as requiring that an infringement defendant be shown to do business "through a permanent and continuous presence" in a jurisdiction in order for venue to be proper in that jurisdiction.**

The rulings by Chief U.S. Judge Leonard Stark of the District of Delaware come on the heels of the U.S. Supreme Court's recent decision strictly interpreting the patent venue statute's residence requirement. [TC Heartland LLC v. Kraft Foods Group Brands LLC, 137 S.Ct. 1514 \(2017\)](#).

In an 8-0 ruling, with Justice Neil Gorsuch not participating, the high court in *TC Heartland* reaffirmed its long-standing position that a domestic corporation "resides" only in its state of incorporation and must have "a regular and established place of business" in order for a patent infringement suit to be brought against it in any other jurisdiction. The court held that the more expansive interpretation of the term "resides" in the general venue statute is not applicable to the patent-specific venue statute.

In the first of the two cases, Judge Stark granted a motion to transfer to the U.S. District Court for the Southern District of Indiana an infringement suit brought by Boston Scientific Corp. against Cook Group Inc., its competitor in the medical device industry. [Boston Scientific Corp., et al. v. Cook Group Inc. 2017 U.S. Dist. LEXIS 146126 \(D. Del. Sept. 11, 2017\)](#).

Cook "appears to have no presence in Delaware whatsoever, let alone a permanent and continuous one," the judge said, noting that

the company has no physical facilities or employees in the state and that none of its "few contacts" with the state amount to a regular and established place of business.

In the second case, Judge Stark found that additional discovery is needed to determine whether generic drug manufacturer Mylan Pharmaceuticals Inc., a West Virginia corporation, has a sufficient presence in Delaware in order for venue to be proper in a suit brought by Bristol-Myers Squibb Co. alleging infringement of its patent for the blood thinner drug Eliquis. [Bristol-Myers Squibb Co. v. Mylan Pharmaceuticals Inc., 2017 U.S. Dist. LEXIS 146372 \(D. Del. Sept. 11, 2017\)](#).

The judge noted that the "Mylan family of companies" has "a nationwide and global footprint" and that Mylan has had "more generic drug applications approved by the FDA over the last two years than any other company." Further, he said, Mylan is a frequent litigant in the Delaware federal court, appearing in more than 100 cases there in the past 10 years. However, he said, there is insufficient evidence in the record to show that Mylan does not have a regular and established place of business in the state and ordered expedited discovery on the issue while the case continues to proceed.

-Lexis Practice Advisor Staff



**RESEARCH PATH:** [Intellectual Property & Technology > Patents > Patent Litigation > Articles](#)







---

## DELAY IN HMDA DATA COLLECTION SOUGHT BY BANKING ASSOCIATIONS, TRADE GROUPS

---

**FIVE NATIONAL TRADE ASSOCIATIONS AND ALL 50 STATE** bank associations are calling for the Consumer Financial Protection Bureau (CFPB) to delay implementation of the Home Mortgage Disclosure Act's ([HMDA](#)) mandatory data collection requirements scheduled to take effect at the beginning of the new year.

Section 1094 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ([Dodd-Frank](#)) amended HMDA and, among other things, expanded the scope of information relating to mortgage applications and loans that must be collected under HMDA, including the ages of loan applicants and mortgagors, information relating to the points and fees payable at origination, the difference between the annual percentage rate associated with the loan and benchmark rates for all loans, the term of any prepayment penalty, the value of the property to be pledged as collateral, the term of the loan and of any introductory interest rate for the loan, the presence of contract terms allowing non-amortizing payments, the application channel, and the credit scores of applicants and mortgagors.

In 2015, the CFPB finalized a rule expanding the data reporting requirements under HMDA. January 1, 2018, is the day of reckoning for complying with the rule.

In July 31 letters to the CFPB, the American Bankers Association, Consumer Bankers Association, Consumer Mortgage Coalition, Housing Policy Council of the Financial Services Roundtable, Mortgage Bankers Association, and the state bankers associations requested a one-year delay that would push mandatory reporting back to January 1, 2019.

To help ease the new reporting burden, the CFPB has published several compliance resources (including most recently in December 2015 and January 2017)—a fact that was acknowledged by the associations. However, the associations said, a delay in the compliance date is still needed.

“Although we greatly appreciate the CFPB’s work to facilitate implementation of this major data collection and reporting rule, the CFPB’s regulatory process and technological framework for this rule are still incomplete. Proposed amendments to the rule are not yet finalized. Moreover, the HMDA data reporting portals, geocoding tools, data validation, and rule edits are not yet issued. All of these items are needed to ensure compliant business process and systems changes by the effective date,” they said.

The associations also raised concerns about the protection of consumer financial data, noting that the CFPB has not yet determined what data will be made publicly available or how it will maintain the integrity of private financial information such as borrowers’ credit scores, debt-to-income ratios, and loan-to-value ratios.

The associations further recommended that institutions be given the option to incorporate new data requirements into their data collection for 2018 on a voluntary basis.

- *Pratt’s Bank Law & Regulatory Report*, Volume 51, No. 9



**RESEARCH PATH:** [Finance > Financial Services Regulation](#)  
[> Financial Institution Activities > Articles](#)



**David J. Goldschmidt and Michael J. Schwartz**

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

# TOP TEN PRACTICE TIPS: PUBLIC COMPANY REPORTING



The planning and preparation that each public company must undertake in connection with periodic and current reporting is substantial in terms of time, effort, and resources. Managing the reporting process can be a daunting task for a company as members from several departments within the organization typically are involved in addition to service providers. A company's internal legal team and outside counsel play critical roles in the reporting process. Below are 10 practice points for attorneys that can help ensure you are best positioned to effectively and efficiently assist with a company's periodic and current reporting.

**1 Familiarize yourself with the rules and know the applicable deadlines.**

It seems simple to say that lawyers need to know the rules; however, there is a broad and complex tapestry of rules and regulations that apply to periodic reporting. The three primary reports that all domestic public companies are required to file are Annual Reports on Form 10-K, Quarterly Reports on Form 10-Q, and Current Reports on Form 8-K. Merely reviewing a form itself is not enough to sufficiently familiarize yourself with the applicable form requirements. The forms direct the user to rules and regulations outside of the form, such as Regulation S-K or Regulation S-X, for much of the substance of the required disclosure. Further, if the company has securities listed on a stock exchange, the stock exchange may have additional requirements for disclosure items to be contained in certain periodic reports of which you must be aware.

In addition to understanding the substance of what goes into each report, it is critical to know when the report is due. Late filings can have a number of implications for a company. A late filing may affect a company's ability to use a short form registration statement on Form S-3 or cause a company to lose its status as a well-known seasoned issuer, each of which could have a significant impact on the company's capital raising activities. Filing delinquencies could also subject a company to liability under the securities laws, including the antifraud provisions; affect the company's ability to remain listed on the New York Stock Exchange or NASDAQ; or trigger a default under the company's debt or other agreements. While a company can plan in advance to meet the filing deadlines for Form 10-Q and Form 10-K, Form 8-Ks, which typically are due within four business days from the applicable triggering event, often can be problematic. Each company must have a process in place to ensure that it can identify when a Form 8-K triggering event occurs and is able to draft and file the report (including any necessary exhibits) by the reporting deadline. Equally important is the ability of outside counsel to quickly advise on (and often flag for the company) triggering events and the correlating reporting requirements.

**2 Stay informed on rule changes, Securities and Exchange Commission (SEC) initiatives, and accounting developments.**

Staying abreast of the latest rule changes, SEC initiatives, and accounting developments is key for providing effective advice on periodic reporting. Identifying changes to the rules is clearly important and timely conveying these changes to relevant parties in the disclosure process is vital. Equally important is staying informed on current SEC initiatives or areas with heightened SEC focus. Staying informed on SEC initiatives and areas of focus will enable your client to address any such changes proactively, avoid SEC scrutiny, and improve the quality of the company's reports. Staying up-to-date can be a challenge, but there are many ways that you can stay current, including reviewing publications by law firms and accounting firms and attending relevant conferences. Finally, changes in accounting rules can affect a company's report beyond the financial statements. Therefore, it is important for counsel to stay current on recent accounting developments and not merely rely on the company's accountants and accounting personnel.

**3 Know your company's business and stay abreast of developments affecting the company.**

The most effective disclosure lawyers have a deep understanding of the company's business and industry. An understanding of the business is important to effectively assist in assessing materiality of business developments and identifying material trends and uncertainties in the business that should be disclosed. Developing a process to stay current in developments within the company and its business is critical to ensuring that the company's reports are accurate and complete. Many companies have a disclosure committee that consists of officers and employees who know the company and its business best. For outside lawyers, when reviewing disclosure in periodic reports, it is a good idea to include diligence questions in your comments to the report to elicit information and prompt discussion. In addition, staying current with political and



macroeconomic events is important, as the effect of such events may be material on a company and should be disclosed.

#### **4 Identify in advance any difficult disclosure issues.**

Periodic reports on Forms 10-K and 10-Q must include not only all required line item disclosures, but also all information otherwise necessary to make required statements not misleading. In addition, Form 8-K disclosure is triggered by unquestionably or presumptively material events that require real-time disclosure. Determining materiality is a facts and circumstances analysis and can be difficult in many instances. In addition, there may be ongoing corporate transactions, regulatory inquiries, or other corporate developments that are sensitive in nature, requiring that the disclosure be carefully crafted or that may not be ripe for disclosure. Identifying difficult disclosure issues and analyzing them without undue time pressure will make it easier to reach the appropriate conclusion on whether disclosure is required and improve the quality of any necessary disclosure.

#### **5 Review disclosure practices of other companies in the same industry.**

You should look at reports filed by comparable companies in the same industry, as they may provide you with valuable insights into how others are addressing the disclosure issues that the company faces. In addition, reviewing the disclosure of others can help identify points of interests for investors, including financial metrics that investors focus on when comparing companies in a particular space. Knowing what a company's competitors are saying about their business and the industry is an important benchmark and can be a very helpful tool in advising a company in its reporting.

#### **6 Involve specialists inside and outside the organization as necessary.**

Certain disclosures included in the company's reports may address topics that are beyond the expertise of the individuals having primary responsibility for preparing and reviewing the reports. For example, if there is a summary of a regulatory regime applicable to the company, it would be prudent to have the company's regulatory experts review the disclosure. In addition, if the company is involved in a material litigation or a material corporate transaction, the company should share the description of the litigation or transaction with the law firm representing them in the matter. This will help to ensure that the disclosure is accurate and complete.

#### **7 Make sure reports reflect the results of any previous comment letters from the SEC.**

The SEC staff is tasked with reviewing each public company's periodic reports at least once every three years pursuant to a Sarbanes-Oxley mandate. As a result of such review, the staff may request changes to the company's disclosure in future filings. Make sure that the staff's comments continue to be reflected in future reports.

#### **8 Create a reporting calendar and communicate the calendar with the relevant participants in the process.**

A reporting calendar can be a useful tool to help management, the company's board of directors (including relevant committees), employees, auditors, and other outside service providers to allocate the necessary resources to the reporting process. In addition to the filing dates, the calendar should include dates for expected



distributions of drafts and the dates on which comments are due from the various participants.

## 9 Plan ahead for obtaining any necessary auditor consents.

Auditors are not required to consent to the inclusion of their audit report in a periodic report. However, when the company has an effective registration statement on file that forward-incorporates the company's periodic and current reports (such as a Form S-3 or a Form S-8), the company will need to obtain an auditor's consent to incorporate the relevant financial statements by reference into the registration statement. If necessary, the consent typically would be filed as an exhibit to the applicable report. You should work with the company's auditors well in advance to ensure that the consent will be delivered timely.

## 10 Don't forget to update the exhibit list.

A common mistake companies often make is failing to update the exhibit list. In connection with the company's annual report, the exhibit list should be updated to remove agreements that are no longer in effect or material to the company and to add any agreements that may not have previously been material but became material or that were entered into in the period covered by the filing. Companies may elect not to file certain agreements as an exhibit to Form 8-K and instead file these agreements with their next periodic report. When electing to do so it is important to remember to file the agreement(s) at the appropriate time. **L**

*David J. Goldschmidt and Michael J. Schwartz are partners in the New York office of Skadden, Arps, Slate, Meagher & Flom LLP. Mr. Goldschmidt represents investment banks and U.S. and international issuers in a variety of financing matters, including public offerings and private placements of debt and equity securities, and international securities offerings. He counsels U.S. and international clients on an ongoing basis, including advising on corporate governance, SEC filings, and disclosure issues. Mr. Goldschmidt also serves on Skadden's Policy Committee. Mr. Goldschmidt is very active in representing and advising real estate investment trusts (REITs) in connection with capital market transactions, including many initial public offerings and general corporate matters. Michael Schwartz represents U.S. and international issuers, private equity and hedge fund sponsors, REITs, and underwriters in a wide variety of public and private finance transactions. He has worked on numerous high-yield and investment grade debt offerings, initial public offerings, spin-offs, and other public and private equity and equity-hybrid securities offerings, as well as debt tender offers, exchange offers, and other refinancing transactions. Mr. Schwartz also counsels corporate clients on an ongoing basis, assisting with the review and preparation of SEC filings, corporate governance matters, and interactions with security holders, stock exchanges, and other regulatory bodies.*

### Related Content

For an overview on the major items of disclosures for Form 10-K, see

#### > **DRAFTING AND REVIEWING FORM 10-K**

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Public Company Reporting > Periodic Reports > Practice Notes](#)

For guidance on preparing Form 10-Q, see

#### > **DRAFTING AND REVIEWING FORM 10-Q**

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Public Company Reporting > Periodic Reports > Practice Notes](#)

For more information on seeking extensions for filings and the consequences of late filings of periodic reports, see

#### > **PREPARING A LATE PERIODIC REPORT**

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Public Company Reporting > Periodic Reports > Practice Notes](#)

For additional details on the periodic and current reporting obligations of public companies, see

#### > **PERIODIC AND CURRENT REPORTING RESOURCE KIT**

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Public Company Reporting > Periodic Reports > Practice Notes](#)

 **RESEARCH PATH :** [Capital Markets & Corporate Governance > Public Company Reporting > Periodic Reports > Practice Notes](#)







Terrance Oben OBEN LEGAL

# NAVIGATING COMPLIANCE CONCERNS



Companies in today's global economy are confronted with growing legal and compliance risks due to the expanded scope, complexity, and global nature of their business activities. Accordingly, companies wishing to avoid these risks are incentivized to build a robust risk-based corporate compliance program that is designed to limit the company's exposure to those risks.

#### **THIS ARTICLE DISCUSSES PRACTICAL STEPS THAT**

companies can take to successfully embed a positive compliance culture and outlines a proposed approach to developing and implementing a compliance program that can be used globally, regardless of industry or the size of your company.

### **Understanding the Compliance Risk Framework**

As a core function of corporate governance, compliance plays an integral role in achieving an organization's primary objective—maximizing shareholder value and protecting company assets. To achieve this objective, companies must deploy sustainable internal and external long-term strategies focused on enduring operational performance, while protecting the interests of their shareholders and other stakeholders.

#### **What Are Compliance Risks?**

Every organization is unique, and so are its costs for doing business. Generally, compliance risks can be viewed as the possibility of present or future loss/damage to an organization's integrity because of a failure (or apparent failure) to comply with laws, regulations, or other applicable business standards. Therefore, compliance risks are business risks—because they require organizations to conduct business activities within a set of prescribed ethical and/or legal boundaries. In the context of this article, damage to an organization's integrity includes legal or regulatory sanctions, financial loss, and damage to reputation, market share, customer base, or contracts.

#### **What Is Compliance?**

Compliance is the process of turning compliance requirements into practical operational control processes.

#### **Where Do Compliance Requirements Come from?**

##### *Litigation – Failures in Corporate Governance*

Compliance requirements have largely been driven by regulatory scrutiny targeting business conduct across the globe, particularly in the wake of several significant corporate financial scandals and the financial crises of 2000 and 2008.

For example, in the early 2000s, the Enron scandal shocked the world when it was revealed that its executives and auditors had defrauded employees and shareholders for years by falsifying financial and accounting records that concealed billions of dollars of debt and failed deals. Enron's eventual bankruptcy, along with other corporate financial scandals (e.g., WorldCom, Qwest) revealed the

need for enhanced corporate governance and ethical conduct by corporations. As a result, the [Sarbanes-Oxley Act of 2002](#) (SOX) was enacted to improve corporate governance by requiring enhanced accountability for public companies and the adoption of a code of ethics for their executives.

The underlying message from enforcement agencies is that companies must develop and implement truly effective corporate compliance programs—ones designed to prevent violations before they occur, or at a minimum, detect and stop any violation quickly.

##### *The U.S. Sentencing Guidelines for Organizations*

Over the years, the Federal Government through the [U.S. Sentencing Guidelines for Organizations](#) (Guidelines) has attempted to influence corporate behavior by establishing a structure that assesses monetary fines for corporate misconduct based on a specific formula. In essence, the Guidelines provide a potential for fine reduction for organizations that implement and maintain an "effective compliance and ethics program." Although the Guidelines don't counsel companies on how to establish an effective compliance program, they do provide a list of several elements that compliance and ethics professionals should ensure that their programs include. Historically, many companies have used these elements, or some form thereof, as a foundation for their corporate compliance programs.

##### *Targeted Legislation*

In addition to the Guidelines, legislation targeting specific conduct in the United States and abroad has also had a tremendous impact on influencing organizations to establish and maintain corporate compliance programs. Examples include legislation targeting bribery and corruption, cybersecurity, financial fraud, terrorist financing, and labor conditions. These regulations have compliance mandates to which organizations must adhere, thereby creating a need for adequate compliance programs.

#### **How Should Your Organization Effectively Manage Compliance Risks?**

Managing compliance risks within your organization does not necessarily need to be complicated, but it often is. This is primarily because duties related to compliance risk management usually reside with numerous teams working together across different business units, departments, regions, and divisions. In order to successfully address this complexity, you must clearly define the essential roles and responsibilities of each participant. This will lead



to a more effective and efficient compliance program. The design and approach of the compliance program will be addressed later in this article.

### **How Would Your Organization Benefit from Implementing a Compliance Program?**

A well designed and implemented compliance program helps a company to preserve and promote its corporate health and values. More specifically, the ultimate benefits of developing an effective compliance program include:

- Preventing violations of law and the potential consequences of violations by:
  - Reducing conflicts of interest
  - Reducing fraud risks
  - Improving accountability
- Reducing liability for misconduct
- Improving company operations by:
  - Implementing stronger internal controls
  - Reducing errors in financial operations
  - Improving records accuracy

- Building stakeholder trust
- Increasing efficiencies and consistencies

### **What Aspects Should Be Considered When Designing the Compliance Program?**

- **Size matters.** The size and complexity of your company's business activities may require differences in the design of your compliance program:
  - Small, less complex vs. firm-wide/multi-locational approach
  - Wide range of applicable rules and standards:
    - Be mindful of potentially conflicting laws across different jurisdictions (e.g., European Union limits on how much personal information data can be transferred across borders that could impact sanctions or anti-money laundering law compliance)
- **Geography matters.**
  - Domestic, regional, or global operations
  - Cultural differences
  - Language difference
- **Incentives matter.** Consider various types of incentives to identify those that will be the most compelling



**THE FIRST STEP IN ESTABLISHING YOUR COMPLIANCE PROGRAM IS TO DEFINE SENIOR MANAGEMENT'S RESPONSIBILITY FOR MANAGING AND OVERSEEING COMPLIANCE RISKS WITHIN THE COMPANY. THIS RESPONSIBILITY IS TYPICALLY SHARED TO VARYING DEGREES AMONG THE BOARD, SENIOR MANAGEMENT, AND THE CORPORATE COMPLIANCE DEPARTMENT.**

### **Before the Program: Compliance, Governance, and Oversight**

Compliance with applicable laws and regulations within a company is everyone's responsibility and should be part of the culture of the company, not just the responsibility of dedicated compliance staff (see Compliance Department section below). That said, the company's governing bodies (i.e., board of directors or equivalent bodies) and senior management play an essential role in encouraging all employees to behave ethically and laying the foundation upon which a company builds its compliance culture.

Therefore, a commitment to a positive compliance culture begins with a strong tone at the top from the most senior levels of the company's management. This tone at the top should be cascaded to middle and lower management levels to help ensure the tone at the top is also the tone in the middle and the tone all the way down to junior employees. This tone should be established both on paper—through policies and procedures—as well as by example, through senior management actions (e.g., verbal emphasis of company's commitment to compliance during business meetings, organization of a compliance summit for key compliance officials, department heads, and senior management).

A corporation's governing bodies and senior management have the primary responsibility and accountability for establishing the organization's objectives (i.e., the reasons the organization was created). Therefore, they must be the ones to define appropriate strategies to achieve those objectives and establish governance structures and processes aligned with those objectives.

Senior management must actively support and engage in the company's compliance efforts and demonstrate that they take compliance seriously. Employees are likely to follow the lead of their superiors. Thus, when senior management sets the right example, compliance is perceived as an integral part of the company's business activities. Since compliance risks are ultimately business risks, a culture of compliance is simply good business.

The suggestions below for the roles and responsibilities assume a corporate governance structure comprised of a board of directors and senior management.

### **Responsibilities of the Board and Senior Management**

The first step in establishing your compliance program is to define senior management's responsibility for managing and overseeing compliance risks within the company. This responsibility is typically shared to varying degrees among the board, senior management, and the corporate compliance department. Jointly they are responsible for establishing and implementing a compliance risk management and oversight program designed to prevent and detect compliance issues, while promoting a strong compliance culture.

#### **The Board of Directors**

The board of directors should take on the following roles and responsibilities:

- Establishing an appropriate culture of compliance and requiring adherence to compliance policies within the company by:
  - Ensuring that the board is familiarized with the compliance risks and challenges related to the company's operations
  - Promoting a culture that fosters strong ethical conduct and compliance with applicable compliance laws
  - Requiring that the company and employees conduct all activities in accordance with both the letter and the spirit of applicable compliance regulations
- Obtaining senior management commitment by ensuring:
  - Management of the compliance risks in a manner that is consistent with the board's expectations
  - Proper ongoing communication of compliance messaging throughout the company through policies, training, and in-person forums
  - The establishment of a corporate compliance department that has a prominent status within the company
- Exercising oversight of the program by:
  - Reviewing and approving key program elements, policies, and projects
  - Overseeing management's timely implementation of the program and resolution of compliance issues
  - Reviewing the effectiveness of the program at least annually

Note that the board's oversight tasks may be delegated to an appropriate board-level committee, such as an audit committee.

### Senior Management

Senior management should take on the following roles and responsibilities:

- Developing and establishing an effective compliance organization with defined responsibilities for managing compliance risks
- Carrying out the board's expectation of embedding a compliance culture within the company by setting a good example, such as by demonstrating an understanding and consistent application of compliance rules
- Supervising and overseeing the implementation of board-approved standards for the company's compliance risk management program
- Reporting directly to the board regarding significant compliance matters and the effectiveness of the program
- Enforcing standards and holding staff accountable for noncompliance
- Ensuring the business and compliance departments are provided with adequate resources to fulfill their mission

Active management support empowers employees to speak up when improper conduct is suspected or identified, so that prompt corrective action can be taken.

### The Compliance Department/Function

The compliance department is a core corporate department, just like Information Technology (IT), Finance, Human Resources (HR), or Marketing. It is responsible for developing and overseeing the implementation and maintenance of the company's compliance program. Before developing the compliance program, you should ensure that your company has an internal corporate compliance department and have a good understanding of its structure. Some common structures include:

- The compliance department within specific operating business lines, a specific region, or locally, for companies with international operations
- Separate units for specialized areas like anti-money laundering and terrorist financing, sanctions and embargoes, and data protection
- The compliance department as one unit

Additionally, as there is a close relationship between compliance risk and certain aspects of operational risk, some compliance responsibilities and activities may be assigned to other departmental units such as audit, finance, IT, HR, or monitoring and testing. In these cases, to ensure proper governance and management of responsibilities, the compliance department will need to incorporate appropriate controls within its structure to account for those risks.

### Related Content

For an outline of a proposed approach to developing and implementing a compliance program, see

#### > [CREATING A COMPLIANCE PROGRAM CHECKLIST](#)



**RESEARCH PATH:** [Commercial Transactions >](#)  
[General Commercial and Contract Boilerplate >](#)  
[Compliance Programs and Risk Assessment > Checklists](#)

For an overview of the risk assessment process, see

#### > [RISK ASSESSMENT](#)



**RESEARCH PATH:** [Commercial Transactions >](#)  
[General Commercial and Contract Boilerplate >](#)  
[Compliance Programs and Risk Assessment > Practice Notes](#)

For a list of the documents that are needed in order to conduct the risk assessment process, see

#### > [CHECKLIST - INFORMATION AND DOCUMENTS TO REVIEW IN A RISK ASSESSMENT](#)



**RESEARCH PATH:** [Commercial Transactions >](#)  
[General Commercial and Contract Boilerplate >](#)  
[Compliance Programs and Risk Assessment > Checklists](#)

Notwithstanding the structure of your compliance department (i.e., stand-alone, local, or within another business unit), an effective compliance department should always include the following characteristics:

**Independence.** The compliance department must be appropriately independent, both in its responsibilities and reporting lines. This independence facilitates objectivity in carrying out its duties, as well as avoids conflicts of interest that may arise as a result of proximity to the company's business lines. Some common factors contributing to independence include:

- Formal status within the company
- Appointment of a head of compliance (i.e., General Counsel / Chief Legal Officer or Chief Compliance Officer)
- Governance of compliance activities (only requiring compliance staff to take on compliance-related responsibilities or adopting additional measures to avoid conflicts of interest where this is not practicable)
- Restrictions on incentive compensation of compliance staff that is related to business performance
- Unfettered access to any employee, information, and/or communication necessary to carry out its responsibilities





**Adequate resources.** In addition, the compliance department should be allocated a ring-fenced budget to carry out its responsibilities. This means that its budget is autonomous, dedicated, and protected—not subject to external diminution by business lines.

**Clearly defined internal responsibilities and reporting.** Roles and responsibilities within the compliance department should be clearly defined. The responsibilities for all stakeholders in the business line and other departments that perform compliance tasks should be defined as well.

Depending on the size, risks, and structure of the organization, reporting lines should be appropriately structured to minimize potential conflicts of interest. Regardless of organizational structure, all company staff should have a clear understanding of appropriate escalation protocols. Best practice is an escalation protocol requiring any employee who suspects or knows of a compliance issue or violation to report this concern to the person to whom he or she directly reports. Importantly, it should be required that the compliance department be simultaneously included in any such reporting so as to ensure that the issue is addressed appropriately. This notification could go to a designated compliance individual or to a designated generic compliance e-mail address.

**Subject to periodic and independent review by internal audit.** Given the critical role that the compliance department plays in the company, it is important to ensure that the department is functioning properly. This can be accomplished by the periodic review of its operations by an independent group within the company, such as the audit department.

## Developing the Compliance Program

All companies, regardless of size, industry, or business, should adopt a formal document (policy, procedure, or standards) that lays out the control framework for the company's compliance program.

The naming conventions used for the compliance program elements discussed below are not prescriptive; neither are the number of elements. Rather they reflect common terminology used in practice. Whatever elements you choose for your compliance program, together they should create an integrated framework or cycle.

### Leadership and Oversight

This element of your compliance program lays out the compliance department's governance and organizational structure. The areas covered in the section should demonstrate the robustness of the compliance organization. This includes addressing independence, resources, roles and responsibilities, and reporting lines.

Be sure to include specific statements related to the following:

- Clearly defining roles and responsibilities of the board, senior management, compliance function (add local and regional compliance if applicable), business unit/operations staff, and internal audit
- Defining protocols for the organization's senior and executive management to resolve or ratify compliance risk management issues
- Establishing documentation requirements to demonstrate adherence to protocols and oversight
- Stating how the company creates a culture of compliance, such as:
  - Expectations for employees to adhere to policies, rules, and standards
  - Compliance embedded in executive management routines and key communications
  - Compliance responsibilities as part of staff's day-to-day activities
- Ensuring the compliance department has an independent position in the company with the ability to enforce compliance policies across the organization
- Ensuring the compliance department participates in key company committees
- Developing an independent quality assurance (QA) program to monitor and oversee effective implementation of and consistent adherence to compliance standards
- Establishing escalation and reporting protocols to report compliance risk matters through appropriate channels:
  - Regardless of organizational structure, all company staff should have clear understanding of appropriate escalation protocols.

Best practice is an escalation protocol requiring any employee who suspects or knows of a compliance issue or violation to report this concern to whom they directly report.

- Importantly, it should be required that the compliance department be simultaneously included in any such reporting so as to ensure that the issue is addressed appropriately. This notification could go to a designated compliance individual or to a designated generic compliance e-mail address.
- Implementing compliance management routines to establish effective oversight of compliance matters
- Establishing a framework for the review and approval of new business initiatives
- Establishing a process for developing annual compliance plans (corporate, business line, or regional)

### Regulatory Management

This element focuses on two things: (1) how you identify new and changing laws, regulations, and standards, including the associated process of communicating the obligations to the business lines and ensuring applicable policies and processes are updated accordingly; and (2) how your company interacts with regulators and coordinates regulatory examinations and inquiries.

#### Regulatory development assessment, notification, and response.

Start by assessing all regulatory updates received through any means (e.g., automated e-mail notification) to determine the applicability and impact to the organization. This process may involve internal consultation with other units (e.g., legal, lines of business, senior management) or with outside parties (e.g., regulators, outside

counsel, or industry groups). Incorporate input and guidance from these consultations into the overall assessment of impact resulting from the regulatory development. Draft and send out regulatory development notices to required audiences (e.g., line of business, region, senior management). A regulatory development may require that the business line conduct an existing exposure review, make changes to existing policies/procedures, conduct internal training, or take other control action as appropriate.

**Interaction and coordination with regulators.** It is important to designate a company point person who will manage interactions with regulators. This person is usually a member of the legal department. If a regulator seeks to conduct an exam or inquiry, legal staff will review the regulatory requirements and create a response plan. Compliance staff should also be involved in this process. It is imperative to have a good relationship with regulators; being responsive and organized, with clear company response protocols helps to achieve this.

Your compliance policy should also address:

- Whose role/responsibility it is to assess regulatory development and address any needed regulatory response
- The processes for monitoring, identifying, tracking, and reporting existing laws and any subsequent developments
- Impact analysis processes, including appropriate mitigating controls
- Processes to manage compliance targeted regulatory events (exams) and inquiries





**EFFECTIVE COMMUNICATION AND TRAINING ARE CRITICAL TO RAISING AWARENESS AND BUILDING A COMPANY'S CULTURE OF COMPLIANCE. THIS, IN TURN, ENCOURAGES EMPLOYEE COMPLIANCE WITH POLICIES AND PROCEDURES NECESSARY TO IMPLEMENT THE CONTROLS REQUIRED BY A COMPLIANCE PROGRAM.**

### **Risk Assessment and Reporting**

Compliance risk assessment is one of the key program components by which your company's overall compliance risks are identified, analyzed, and measured. Therefore, it is important that a consistent approach is established. The effectiveness of your entire compliance program is driven by the results of the risk assessment as it helps to:

- Understand the impact and level of compliance risks by the business lines
- Facilitate the reporting of compliance risks to stakeholders
- Form the basis for prioritization of resource allocation in the business and for annual compliance plans, including risk-based training, risk-based monitoring, and testing plans

The following steps should be taken:

- Identify key compliance risks associated with business activities and regulatory requirements
- Identify the business line processes, systems, policies, and procedures that define the mitigating controls
- Conduct risk assessments of business units through evaluation of inherent risk and effectiveness of the controls
- Develop a process for consistent measurement of inherent risk and assessment of controls within a defined residual risk matrix and completion of compliance risk assessments for each business unit
- Communicate risk assessment ratings to key business stakeholders
- Report on the management of compliance risks, significant issues, and key risk indicators
- Report compliance risk within established categories and reporting hierarchies

### **Training and Communication**

Once you have identified your company's risk exposure, you can then take steps to promote staff awareness of those risks. Effective communication and training are critical to raising awareness and building a company's culture of compliance. This, in turn, encourages employee compliance with policies and procedures necessary to implement the controls required by a compliance program.

Compliance training should be risk-based in order for it to be relevant and effective and should involve input from business line stakeholders.

There are generally three types of compliance training that you can implement. The best approach will depend on your company's particular circumstances:

1. Company-wide and cross-business line compliance training
2. Business line-specific compliance training –or–
3. Compliance department training for compliance staff

In either instance, regardless of the selected training approach, you should:

- Conduct a compliance training needs assessment—to identify and evaluate the compliance requirements for employees:
  - Prioritize training and awareness based on risk evaluation (i.e., impact to business and risk assessment results)
- Develop and communicate training plans to key business stakeholders:
  - Coordinate with business stakeholders on topics, audience, and delivery methods
  - Include a training strategy and a communications plan
- Develop training content for training topics
- Track and report on training completion:
  - Track and report training delivery, attendance, and noncompliance
- Periodically evaluate the effectiveness of compliance training modules and awareness efforts through course feedback

It is important to consider the factors that are unique to your audience during the development stage of your training. Factors like geography and culture can greatly influence the way the training is received. For instance, the age demographic of staff, as well as other factors, at a start-up company may lead to a certain attitude towards compliance training and a certain rate at which they consume the compliance information. This could be completely different for a more mature business line. Thus, implementing the same training

## Related Content

For a high-level listing of topic categories to review when conducting a risk assessment, see

### > [CHECKLIST - POTENTIAL TOPICS TO REVIEW IN A RISK ASSESSMENT](#)



**RESEARCH PATH:** [Commercial Transactions >](#)

[General Commercial and Contract Boilerplate >](#)

[Compliance Programs and Risk Assessment > Checklists](#)

For a framework of the interview questions that should be asked during the risk assessment process, see

### > [CHECKLIST- 15 SAMPLE QUESTIONS WHEN PERFORMING A RISK ASSESSMENT](#)



**RESEARCH PATH:** [Commercial Transactions >](#)

[General Commercial and Contract Boilerplate >](#)

[Compliance Programs and Risk Assessment > Checklists](#)

For an explanation of the seven core elements that must exist in order for a compliance program to be deemed effective, see

### > [US SENTENCING GUIDELINES - BENCHMARK FOR AN EFFECTIVE COMPLIANCE AND ETHICS PROGRAM](#)



**RESEARCH PATH:** [Commercial Transactions >](#)

[General Commercial and Contract Boilerplate >](#)

[Compliance Programs and Risk Assessment > Practice Notes](#)

to both groups would be ineffective at achieving the desired engagement. The same can be said for different business industries.

Ultimately, to achieve high participation and retention rates, you should ensure that compliance training is relevant to the business unit being trained with respect to style, content, presentation, and tone. An easy way to achieve this is by involving relevant business stakeholders from the very beginning. Think of it as building compliance training for the business, by the business.

## Policies and Procedures

Your compliance department should mandate the adoption and implementation of appropriate compliance risk management controls in the form of compliance policies and procedures reasonably designed to support compliance with applicable compliance obligations, business requirements, and industry best practices. Compliance policies are also driven by the results of the risk assessment.

The following policy management factors should be incorporated into this component of the compliance program:

- Policy life cycle definition—creation, periodic review, approval procedures, communication, recordkeeping, and archiving
- Form and content requirements—identification of regulatory requirements, risk rationale, controls, and accountabilities
- Ongoing maintenance process

## Monitoring and Testing

Risk-based monitoring and testing are critical elements of an effective compliance program. Monitoring and testing are necessary to evaluate whether compliance risk mitigating controls work as intended, and whether deficiencies are identified and addressed to maintain an effective internal control framework. The scope and frequency of these activities will be determined by the business impact and risk assessment results.

### *Compliance Monitoring*

Compliance monitoring is defined as independent ongoing review of data, reports, and other activities to oversee compliance with regulatory obligations. Compliance monitoring activities are one of the ways that the compliance department independently oversees processes that are implemented across the company for effective mitigation of key compliance risks.

Monitoring activities may include the following:

- Surveillance (e.g., use of models, applications, and/or systems to review, analyze, and flag exceptions or items requiring further review on an ongoing basis)
- Performance oversight (e.g., compliance department review of selected business line activity reports to evaluate process or performance issues on an ongoing basis)
- Review, analysis, and trending of selected business and/or compliance scorecards (key performance or risk indicators) and supporting activities for changes or unusual trends (e.g., areas of the company identified as being higher risk should be monitored quarterly vs. annually)
- Ongoing assessment of business activities such as completing pre-transaction or post-transaction reviews or other quality control or QA activities

### *Compliance Testing*

Compliance testing is a risk-based, independent point-in-time review of policies and procedures, controls, or data sources used for managing compliance risk to assess the effectiveness of the compliance control environment.

In line with the annual compliance plan you established above, your company should also develop a rolling 12-month monitoring and testing plan. As monitoring and testing tasks involve business operations, input from relevant stakeholders should include business management, internal audit, and compliance staff.



The most successful monitoring and testing plans:

- Are developed with consideration of the compliance risk assessment results
- Clearly define monitoring activities and expectations
- Establish compliance testing approach, testing time frames, planning, methodology, and documentation
- Are dynamic, subject to revision due to risk profile changes resulting from significant strategic/business/regulatory changes, emerging risks, industry/market events, and/or other internal/external factors –and–
- Document at a high level the compliance monitoring and testing activities planned for the next 12-month period

### Issue Management

Finally, your compliance program should also establish proactive protocols for compliance-related issue management and resolution. This includes communication of key compliance risks to senior management and mechanisms for review, reporting, and remediation of compliance issues. Due to the structure of some companies, this component may be addressed as part of a different element of the program.

Regardless of whether this component is standalone or not, issues resulting from compliance testing, exams, audits, and self-

assessments are ordinarily recorded, actioned, and reported through some standardized issue management process.

For issue management, the compliance department's standards and protocols for effective communication and resolution of compliance risk management issues require:

- Identification, documentation, and timely resolution of compliance issues, as well as a framework to enable holistic reporting of issues regardless of the source of identification
- Criteria for documenting and resolving issues in accordance with the organization's risk governance framework
- Designated roles and responsibilities for documentation and remediation activities
- Expectations for root cause analysis

### Suggested Implementation Approach

Depending on the size of your organization, there may already be a team that is responsible for implementing change activities. Regardless, implementation of a compliance program is a huge effort and should be carefully planned out. Depending on the complexity of the plan, your company may benefit from adopting a formal implementation guide. Such a guide should be developed with input from the affected business line management to ensure buy-in and preparedness.

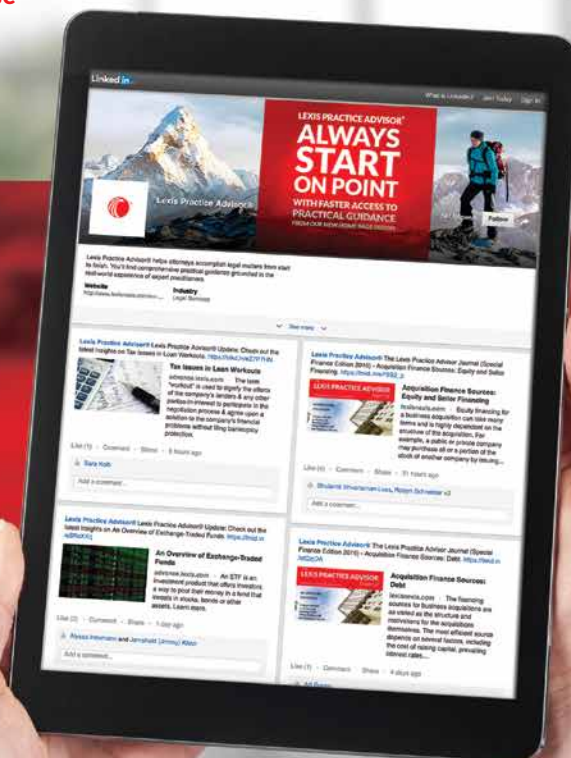


### Lexis Practice Advisor® on LinkedIn® Product Showcase

**“FOLLOW” MORE  
THAN FRIENDS  
AND COLLEAGUES**



**Put LinkedIn® to work for your practice, too**  
Lexis Practice Advisor® on LinkedIn highlights the latest insights and guidance written by expert attorney authors on the topics that matter most to your practice.



Make “following” count—Follow Lexis Practice Advisor on LinkedIn  
[WWW.LEXISNEXIS.COM/PRACTICE-ADVISOR-LINKEDIN](http://WWW.LEXISNEXIS.COM/PRACTICE-ADVISOR-LINKEDIN)

In general, implementation will involve careful consideration of the following:

- Definition of owners and governing process (i.e., what person or business unit owns which part of the implementation process for which they will be responsible for responding to questions, etc.)
- Development of a communications strategy
- Conducting a gap assessment (i.e., ensure that each business unit is equipped to implement the compliance program and assess current protocols vs. what the compliance program prescribes. This may require negotiating an appropriate solution—there must be agreement on the ultimate implementation plan regarding timing, responsibility, etc.)
- Defining business change requirements (i.e., based upon the gap assessment, determine what costs, human resources, etc. are required to achieve compliance.)
- Building and deploying the implementation plan
- Defining and developing technology solutions (e.g., a project management tool may assist with implementation)
- Measuring, reporting, and tracking (i.e., metrics reflecting the success of the implementation. Set clear goals for each business unit and corresponding progress reporting expectations to ensure

implementation stays on track. The above technology solutions may assist with this process.)

What this looks like for your company will vary. Ideally, you want a phased approach with a pre-determined timeline. Below are high-level aspects of an implementation guide to help you as you consider what yours should entail.

**Purpose.** A simple purpose statement is helpful to those stakeholders not familiar with the project. The purpose statement accomplishes three things:

- Introduces the underlying program being implemented
- Provides a high-level description of the underlying program
- Explains the goal that the structured implementation guide seeks to accomplish

**Scope.** The guide should clearly identify the group or groups of employees or entities responsible for implementing the underlying program.

**Roles and responsibilities.** Because there may be numerous teams responsible for the implementation of the program, or parts of it, the guide should clearly define the roles and tasks for which each of these groups is responsible.





**Communications strategy.** The teams involved must carefully craft a plan for communicating both the principles of the underlying program and its implementation aspects to the rest of the company. Communication is key to keeping everyone apprised of the change process, as well as its impact and company expectations. That way, all stakeholders understand their roles, their commitments,

and implications for inaction. The communication phase should be ongoing, not limited to a set period of time (e.g., weekly communications to company employees highlighting compliance risks). At a minimum, the communications strategy should consider what communications are needed, the method of such communications, and the intended audience in each case.

IMPLEMENTATION PHASES	
<b>PHASE I: IMPACT / GAP ASSESSMENT</b>	<b>Timing: 3 months</b> —depending on factors like size, complexity, and geography of the company
The new program requirements are mapped with the current state of the businesses to determine gaps in their programs.	
<b>PHASE II: DEVELOPMENT OF IMPLEMENTATION PLANS</b>	<b>Timing: 6 months</b> —again, depending on factors like size, complexity, and geography of the company. In this phase, the compliance professionals work with business management to define the appropriate actions needed for the program to be implemented fully.
<ul style="list-style-type: none"> <li>■ In this phase, the compliance professionals work with business management to define the appropriate actions needed for the program to be implemented fully.</li> <li>■ Note: This phase will involve continuous support from the legal and compliance departments in order to accurately define the actions needed for successful implementation. Issues may arise that had not been anticipated, requests for exemption from certain parts of the program by some groups may be considered, and other points of frustrations are common. Your goal is to facilitate the transition and to help the business understand that you are a partner in the process, there to provide the support they need to successfully adopt the compliance program.</li> </ul>	
<b>PHASE III: DOCUMENTATION</b>	<b>Timing: 1 month</b>
In this phase you should gather all completed implementation plans and maintain a single data repository	
<b>PHASE IV: ONGOING OVERSIGHT / MEASURE</b>	<b>Timing: Open</b>
As implementation is completed across the company, the internal audit group may be assigned to conduct onsite reviews of the implementation to ensure that the stated activities and requirements of the program have been successfully adopted and implemented. Any issues should be reported via the outlined issue management processes. For all processes, it may be beneficial to create visual contextual process maps or models, as these are proven to facilitate understanding and assimilation .	

**Terence Oben, Esq.** is Managing Counsel at Oben Legal in New York, NY. His practice focusses on corporate governance, ethics, and compliance, assisting domestic and multinational organizations in a variety of industries design, develop, and implement programs and strategies that ensure decision-making, resource allocation, and business activities are aligned with appropriate ethics and compliance considerations for the organization's circumstances. Mr. Oben designs a variety of management mechanisms and tools that organizations use to operationalize legal requirements and integrate ethics into practices. [www.obenlegal.com](http://www.obenlegal.com)



**RESEARCH PATH:** [Commercial Transactions > General Commercial and Contract Boilerplate > Compliance Programs and Risk Assessment > Practice Notes](#)



**Stephen R. Martin** ARNOLD & PORTER KAY SCHOLER LLP

# Conducting a Risk Assessment

## What is a Risk Assessment?

A risk assessment is a review undertaken to help an organization understand its business and manage the related strategic, operational, financial, and/or compliance risks. In the compliance context, U. S. regulators expect companies to conduct periodic and/or targeted assessments in order to assess and address the legal and regulatory risks that the company faces in its operations and/or activities. A well-devised risk assessment process assists companies in identifying specific vulnerabilities and provides the opportunity to mitigate those risks that are most likely to occur. When undertaken as part of a corporate compliance program, the risk assessment can help business leaders effectively manage and mitigate the organization's legal and regulatory risk.

## Why Conduct a Risk Assessment?

Government regulators increasingly expect companies to undertake a risk assessment process to ensure that the underlying elements of the compliance program are appropriate to the size and complexity of the organization as well as the type, scope, and location of the business venture and its activities. The U.S. Sentencing Guidelines, U.K. Bribery Act of 2010, and the Organisation for Economic Co-operation and Development (OECD) guidelines all have identified the risk assessment process as an essential step in developing a strong compliance program and implementing adequate procedures, particularly with regard to anti-corruption and anti-bribery efforts. The U.S. Department of Justice and the Securities and Exchange Commission clearly stated their expectation, in their joint November 2012 Resource Guide, that corporate compliance programs should be tailored to the "company's specific business and to the risks associated with that business." The tailoring process requires periodically assessing the organization's specific activities, undertakings, ethical culture, industry, and business sector in order to identify relevant risks and gaps in the management of those risks. Particularly for companies operating in a complex, fast-moving



and increasingly interconnected environment, it is essential to have a dynamic, risk-based corporate compliance program that evolves with the internal and external environment.

## Scoping the Risk Assessment

When scoping the risk assessment, legal and/or compliance professionals should consider the jurisdictions in which the company operates, the range of company products and services, the entity structure of the organization (including owned or operated entities, joint ventures, and other partnerships in which the company has a majority or controlling interest), government touchpoints, third-party relationships, the sales/business model, strategic business initiatives, and global expansion plans.

The risk assessment should be used to understand the organization's overall risk profile as well as to identify and prioritize the concerns that threaten short- and long-term compliance with applicable laws. Depending on the size and complexity of the operations, a company may choose to conduct an enterprise-wide risk assessment to understand the baseline risk profile and then conduct more focused



**PRIOR TO BEGINNING THE RISK ASSESSMENT, THE COMPANY SHOULD CONSIDER WHETHER THERE IS A STRONG NEED TO PRESERVE THE ATTORNEY-CLIENT PRIVILEGE REGARDING THE ASSESSMENT FINDINGS, PARTICULARLY IF THERE IS CONCERN ABOUT POTENTIAL MISCONDUCT OR ONGOING OR THREATENED LITIGATION, AND/OR IF REGULATORS HAVE INDICATED THE INDUSTRY OR SECTOR IS UNDER SCRUTINY.**

assessments of specific activities and/or jurisdictions based on identified risks and strategic priorities.

The risk assessment should consider current and potential compliance risks, including systemic, organizational, or industry-specific risks and any other unique risks. In its guidance to the U.K. Bribery Act of 2010, the Ministry of Justice suggests reviewing five categories of risk: country, sectoral, transaction, business opportunity, and business partnership risk. For example, a country-specific anti-corruption risk assessment might consider the perceived level of corruption in a jurisdiction, whether there is transparency in governance, and/or legislative support of anti-corruption laws.

The assessment should also consider how existing operations and internal controls contribute to risk, such as inadequate procedures and/or poorly applied internal controls. By reviewing these categories of risk, the company will be able to identify areas of the operation that pose the greatest risk of non-compliance with legal obligations and/or company policy.

After assessing whether there is a regulatory compliance risk, the company should determine the level of likelihood that criminal conduct will occur as well as the nature and seriousness of the possible criminal conduct. The likelihood analysis should consider the nature of the business and the history of prior misconduct in the organization or within the industry sector. Government regulators expect that the compliance program will address the most serious conduct that is likely to occur.

### **Who Conducts the Risk Assessment?**

The risk assessment can be conducted internally, by external resources, or through a combined effort. Some companies engage external professionals in order to ensure there is an unbiased review of the compliance risks and the company's practices; other organizations may supplement internal reviews with periodic assessments by external specialists who can assess the compliance risks and/or program gaps in light of best practices and enforcement trends.

Prior to beginning the risk assessment, the company should consider whether there is a strong need to preserve the

attorney-client privilege regarding the assessment findings, particularly if there is concern about potential misconduct or ongoing or threatened litigation, and/or if regulators have indicated the industry or sector is under scrutiny. Management may wish to consult with legal counsel regarding the benefits of preserving the attorney-client privilege and how to preserve the privilege.

Regardless of who conducts the assessment, senior management should communicate with key stakeholders and departments regarding the importance of the risk assessment process to the organization and ensure that the risk assessment team has adequate resources. In assessing whether the risk assessment process is appropriate and/or proportionate to the organization's size and complexity, senior leaders should consider whether the scope of the assessment and the resources allocated towards it compare favorably with other internal assessment processes.

### **Performing the Risk Assessment**

There are four basic steps in conducting the risk assessment: (1) gather and review information, (2) interview key stakeholders, (3) review and evaluate identified risks, and (4) document and report the findings and recommendations for enhancement of the compliance program.

#### **Gather and Review Information**

To begin, the risk assessment team will want to gather key information about the business operations and practices as well as existing compliance materials. In particular, the risk assessment team should gather information about the company structure and locations, industry sector, client base, third-party engagement, policies and procedures, systems and controls, training protocols, audit reports, and compliance monitoring. These materials will assist the team in ensuring that the risk assessment is appropriately scoped by identifying relevant business practices and related risks that may impact compliance obligations.

#### **Interview Key Stakeholders**

For the second step, the risk assessment team should develop targeted questionnaires and/or surveys based on the



organization's operations and the identified compliance risks. A successful assessment will use open-ended questions to elicit objective information about areas of concern and opportunities for enhancement of the organization's compliance risk management.

The team should identify key stakeholders who have knowledge of the company's operations, its actual practices, and the compliance culture. This target list will vary based on the business sector, size of the operations, and scope of the risk assessment, but should include individuals across the operations, including business team personnel, legal, finance, internal audit, and the senior manager responsible for compliance oversight. The risk assessment team should also consider the best format for eliciting actionable information. While focus groups, group interviews, and surveys may capture information from many participants in a short period of time, individual interviews may allow employees to be more candid, to provide more details and context, and/or to describe evolving or emerging issues.

#### **Review and Evaluate Identified Risks**

The third step is to review the findings and evaluate the compliance risk in light of the relevant laws, company policy, and other applicable standards. Particularly for companies with global operations, it is important to understand the impact of international standards and extra-territorial laws on these operations. If needed, the risk assessment team should consult

with subject matter experts and internal or external legal counsel for the local jurisdiction to ensure a full understanding of best practices, the legal framework, and the regulatory environment.

#### **Document and Report the Findings and Recommendations for Enhancement of the Compliance Program**

The final step in the risk assessment process is to document and report the findings and develop recommendations for enhancement of the compliance program. The risk assessment team should carefully compile its findings—including the risk profile, red flags, priority risk areas, and recommendations—in a comprehensive, practical report. In order to facilitate the implementation of appropriate program enhancements, the risks should be ranked according to the likelihood of occurrence as well as potential severity and impact. The report should also identify any areas requiring further assessment and a timetable for updating the risk assessment. The full report should be presented to the general counsel and/or chief compliance officer for consideration of appropriate program enhancement actions. A summary report can be prepared for other key stakeholders, including senior management, the board of directors, and relevant business units and departments.

#### **Building on the Risk Assessment**

Once the company understands the specific compliance risks, red flags, and priority risk areas, the risk assessment findings



## Related Content

For a list of items that should be reviewed when conducting a risk assessment, see

### > [CHECKLIST - INFORMATION AND DOCUMENTS TO REVIEW IN A RISK ASSESSMENT](#)



**RESEARCH PATH:** [Commercial Transactions > General Commercial and Contract Boilerplate > Compliance Programs and Risk Assessment > Checklists](#)

For a set of seven benchmarks to follow in setting up a compliance and ethics program, see

### > [U.S. SENTENCING GUIDELINES - BENCHMARK FOR AN EFFECTIVE COMPLIANCE AND ETHICS PROGRAM](#)



**RESEARCH PATH:** [Commercial Transactions > General Commercial and Contract Boilerplate > Compliance Programs and Risk Assessment > Practice Notes](#)

For sample guidelines for a corporate compliance program, see

### > [SAMPLE CORPORATE COMPLIANCE PROGRAM GUIDELINES](#)



**RESEARCH PATH:** [Commercial Transactions > General Commercial and Contract Boilerplate > Compliance Programs and Risk Assessment > Forms](#)

For details on creating a compliance program, see

### > [CREATING A COMPLIANCE PROGRAM](#)



**RESEARCH PATH:** [Commercial Transactions > General Commercial and Contract Boilerplate > Compliance Programs and Risk Assessment > Practice Notes](#)

For an outline of a proposed approach to developing and implementing a compliance program, see

### > [CREATING A COMPLIANCE PROGRAM CHECKLIST](#)



**RESEARCH PATH:** [Commercial Transactions > General Commercial and Contract Boilerplate > Compliance Programs and Risk Assessment > Checklists](#)

can be used to improve management of compliance risk. The U.S. Federal Sentencing Guidelines advise companies to use the assessment to “design, implement, or modify” the compliance program. The OECD also advises that the risk assessment should be the basis for effective internal controls. Similarly, in its guidance to the U.K. Bribery Act of 2010, the Ministry of Justice suggests that program priorities, resources, and controls should be based on the results of a risk assessment.

The risk assessment findings should also be used to develop an appropriate risk-based auditing, monitoring, and response program, including:

- A risk-based audit plan of specific transactions, business units, processes, countries, and/or market sectors
- Real-time monitoring to identify and address compliance program gaps on an ongoing basis –and–
- Protocols for monitoring and assessing the implementation of risk mitigation plans

By implementing appropriate auditing and ongoing monitoring processes, the company will have another method by which to identify compliance risks and/or improper practices.

## Updating the Risk Assessment

After an initial (baseline) risk assessment is completed, periodic risk assessments should be conducted—either annually or on a schedule proportionate to the organization’s risk profile. The risk assessment is a preventive measure and should be a regular and systemic part of compliance efforts rather than an occasional, ad hoc exercise cobbled together when convenient or after a crisis. Enforcement trends and government priorities change rapidly, so it is vital to stay up-to-date by conducting regular assessments. In this way, the organization can demonstrate that the compliance program adequately and effectively addresses the changing risks facing the business.

## Conclusion

Organizations should document the compliance program enhancements implemented as a result of the risk assessment. Additionally, the findings from periodic risk assessments should be used to assess the effectiveness of the compliance program improvements. Remember that the risk assessment is just the start of the risk management process: the ultimate goal is to use the assessment findings and analysis to reduce or mitigate compliance risk to protect the organization from government scrutiny and enhance the profitability of the enterprise. **L**

*Stephen R. Martin is a partner in Arnold & Porter’s Denver office and focuses his practice on global compliance matters, risk assessment and management, and advising companies in connection with corporate internal and governmental investigations.*



**RESEARCH PATH:** [Commercial Transactions > General Commercial and Contract Boilerplate > Compliance Programs and Risk Assessment > Practice Notes](#)

# Checklist - 15 Sample Questions When Performing a Risk Assessment

This checklist includes key themes from the compliance program expectations of government regulators around the world and best practices broken into five essential elements of corporate compliance that should be present in every company's compliance program: (1) Leadership; (2) Risk Assessment; (3) Standards and Controls; (4) Training and Communication; and (5) Monitoring, Auditing, and Response. This framework serves as the structure for the interview questions listed below. (This is a limited sample set of questions. Actual questions and follow-up queries posed in a risk assessment should be based on the scope and focus of the risk assessment, the company's industry and/or business sector, the level and position of the interviewee, and information gathered from the review of internal documents.)

## Leadership

1. How would you evaluate or describe the tone at the top of the organization?
2. How does the company communicate about the compliance program and/or compliance values?
3. Does the company take compliance seriously? Are there adequate resources?

## Risk Assessment

4. Does the company have an assessment process for identifying risks? Describe the process.
5. What types of compliance risks exist in the operating market(s)? How severe are these risks?
6. Do you agree or disagree with the top risks that have been identified by management?

## Standards and Controls

7. How are the risks to the organization currently managed?
8. Are you familiar with the policies and/or procedures for the following transaction and/or activities? *[Review of key activities or transactions based on the company profile.]*
9. How would you evaluate or describe the company policies regarding compliance?

## Training and Communication

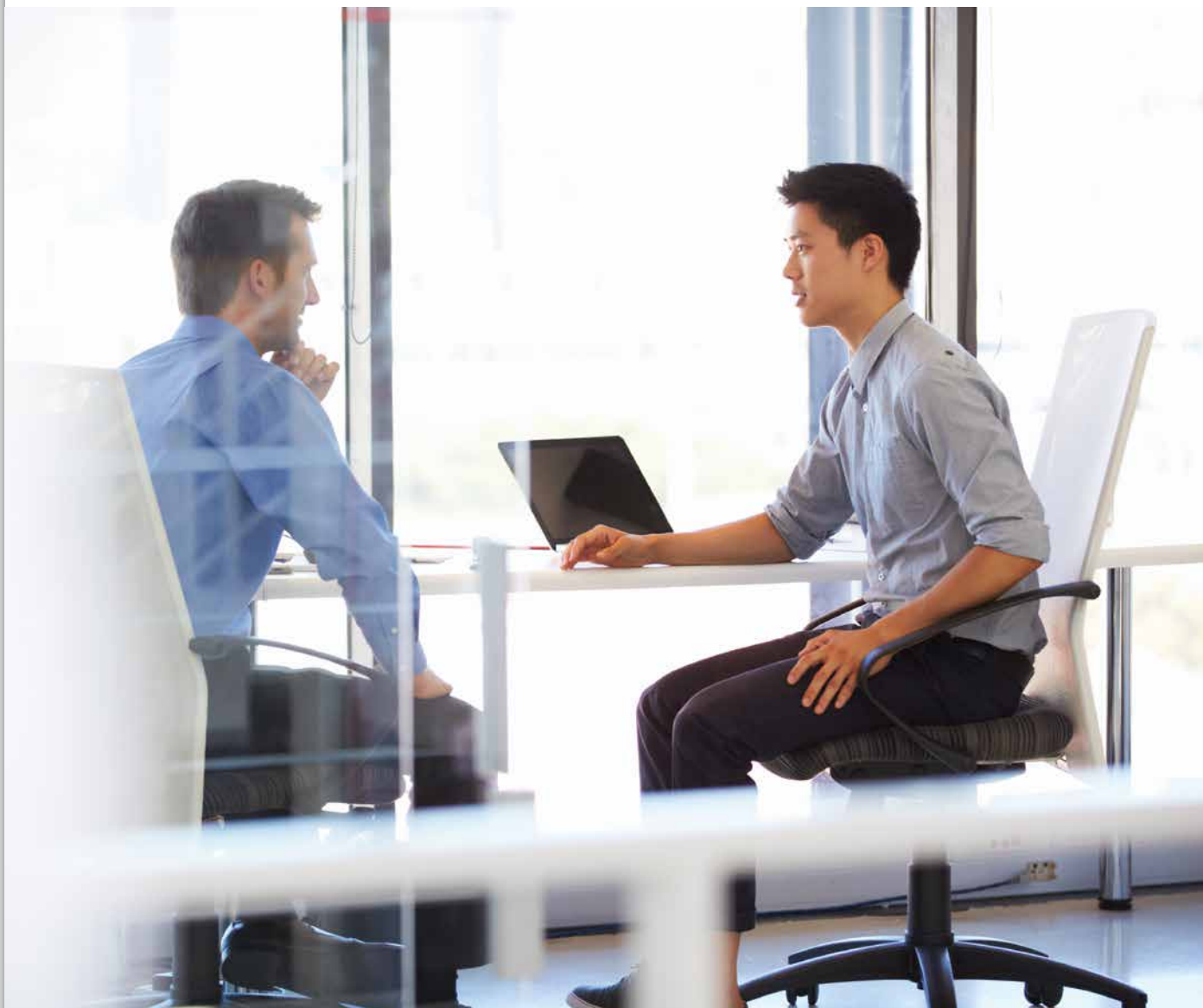
10. What type of training and/or communications do employees receive regarding compliance risks?
11. Was the training relevant to your job responsibilities and compliance risks? Are the training materials adequate?
12. Is there compliance messaging available in your office/location?





## Monitoring, Auditing, and Response

13. What is the culture of reporting issues in the workplace? Do you think people are generally comfortable doing so? Do you think employees fear exposure from, or retaliation due to, compliance reporting?
14. Has the company completed compliance audits? Please describe the process and significant audit findings.
15. When is senior management updated on legal compliance issues? Do they receive written reports or oral briefing? How frequently do updates occur?



---

Checklist provided by [Stephen R. Martin](#), partner at Arnold & Porter Kaye Scholer LLP

---

 **RESEARCH PATH:** [Corporate Counsel > Compliance, Risk Assessment and Governance > Compliance Programs and Risk Assessment > Checklists](#)



**Karen Y. Cho** MORGAN, LEWIS & BOCKIUS LLP

# Key Issues Employers Should Consider when **Integrating Robotics and Automation in the Workplace**

It is indisputable that technology is dramatically changing the way we live in the 21st century and will continue to play an even greater role. The Pew Research Institute's 2014 Future of the Internet survey uncovered wide agreement that robotics and artificial intelligence will permeate most aspects of daily life by 2025, including health care, transportation, customer service, and home maintenance.<sup>1</sup> Yet when it comes to the workforce, experts disagree as to whether technology will ultimately create or displace more jobs.

## **OF THE 1,896 EXPERTS SURVEYED BY THE PEW RESEARCH**

Institute, 48% envisioned a future in which robots and related technologies displaced blue- and white-collar workers, leading to further income inequality and unemployment.<sup>2</sup> However, 52% of experts responded that even if robots took over human jobs, technology would lead to the creation of new jobs and industries.<sup>3</sup> Other studies have painted a similar picture, such as Oxford's 2013 study, which indicated that 47% of American jobs are at "high risk" of being taken over by computers in the next 10 to 20 years.<sup>4</sup> Experts indicate that industries hit the hardest may include automotive, manufacturing, and food services.<sup>5</sup>



<sup>1</sup> Aaron Smith & Janna Anderson, *AI, Robotics, and the Future of Jobs*, Pew Research Center (August 6, 2014), available at <http://www.pewinternet.org/2014/08/06/future-of-jobs/>. <sup>2</sup> Smith, et al., *supra* note 1. <sup>3</sup> Smith, et al., *supra* note 1. <sup>4</sup> Carl Benedikt Frey & Michael A. Osborne, *The Future of Employment: How Susceptible Are Jobs to Computerisation?* University of Oxford (Sept. 17, 2013), available at [http://www.oxfordmartin.ox.ac.uk/downloads/academic/The\\_Future\\_of\\_Employment.pdf](http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf). <sup>5</sup> Christie Nicholson, *Our Rising Robot Overlords: What Is Driving the Coming Upheaval* (August 24, 2011), available at <http://www.zdnet.com/article/our-rising-robot-overlords-what-is-driving-the-coming-upheaval/>.



**ONGOING TECHNOLOGICAL DEVELOPMENTS IN AREAS SUCH AS ROBOTICS AND AUTOMATION COULD HAVE A POTENTIALLY SIGNIFICANT IMPACT ON SEVERAL AREAS OF LABOR AND EMPLOYMENT LAW. . . . THESE TECHNOLOGIES MAY IMPROVE OPPORTUNITIES FOR INDIVIDUALS IN THE WORKFORCE, BUT THEY ALSO MAY LEAD TO WIDESPREAD DISPLACEMENT OF CERTAIN WORKERS AND NEW AREAS OF LIABILITY.**

Even though the full impact of robotics and automation on the workplace may be unknown, one thing is certain—employers should be aware of potential legal landmines and start planning now. This article focuses on areas of employment law that may see the biggest impact and key issues employers should consider when integrating these new technologies.

### **Examples of Robotics and Automation**

Robotics and automation are beginning to impact a wide swath of industries. Self-driving vehicles from cars to autonomous electric long-haul tractor trailers continue to receive widespread coverage. Many transportation companies and automobile manufacturers are committing significant resources to developing and rolling out these technologies. Last year the White House predicted that automation may eventually replace 1.3 to 1.7 million heavy and tractor-trailer truck-driving jobs.<sup>6</sup> Manufacturing is another area where workers are already commonly working beside robots and automated technology. Retailers even use robots to quickly and efficiently fulfill and ship online orders.<sup>7</sup>

But robots are not just taking on manual labor and manufacturing roles; they are also performing human resource-related tasks, such as conducting job interviews and acting as customer service representatives.<sup>8</sup> The medical field has also seen an influx of robots performing neurological, orthopedic, and general surgery—and even reducing surgical complications by up to 80%.<sup>9</sup> Without question, robotics and automated technology are permeating many industries, and they will continue to do so in the years to come.

### **Potential Issues of Workplace Compliance**

Ongoing technological developments in areas such as robotics and automation could have a potentially significant impact on several areas of labor and employment law. In some ways, these

technologies may improve opportunities for individuals in the workforce, but they also may lead to widespread displacement of certain workers and new areas of liability.

#### **Wage and Hour**

Several areas of wage and hour law are likely to be impacted by technological advancements in robotics. With the incorporation of robots, more employees may be able to perform their jobs remotely through telemanipulation. Employees may perform jobs by controlling robots or automated systems from different rooms, worksites, states, or even countries than where the robot is physically located. However, when workers perform their jobs remotely there can be wage and hour consequences. Most employees in the United States are covered by federal employment laws, such as the Fair Labor Standards Act<sup>10</sup>, in addition to the wage and hour laws implemented by many states and municipalities. Generally, the law of the state where the work is performed applies. For example, the California Supreme Court has held that even when an employee may live and work primarily out of state, California's wage and hour laws may apply when the employee performs work within the state for an entire day.<sup>11</sup> Employers may now have to ensure compliance with employment laws in additional, or even multiple, jurisdictions for the same employee within a given pay period. If employees travel consistently and work remotely, this could further complicate the application of employment laws. As remote work trends develop, perhaps an argument can be made that the location of the robot is where the physical work is actually being performed.

These technologies will also likely create jobs where employees have substantial downtime (e.g., an employee simply oversees a robot performing its job and only has to respond when an error occurs.) In theory, remote employment could substantially reduce the amount of compensable time worked

6. Alana Semuels, *When Robots Take Bad Jobs*, THE ATLANTIC (February 27, 2017), available at <https://www.theatlantic.com/business/archive/2017/02/when-robots-take-bad-jobs/517953/>; 7. Sam Sheard, *Amazon Now Has 45,000 Robots in its Warehouses*, BUSINESS INSIDER (Jan. 3, 2017), available at <http://www.businessinsider.com/amazons-robot-army-has-grown-by-50-2017-1>; 8. See, e.g., Cameron Scott, *As Robots Evolve the Workforce, Will Labor Laws Keep Pace?* Singularity Hub (Mar. 16, 2014), available at <https://singularityhub.com/2014/03/16/robots-entering-the-workforce-but-are-labor-laws-keeping-up/> (discussing "Sophie" the human resources interviewing robot that measures interviewees' "psychological responses" to questions, such as their eye movement, along with their verbal answers); see also News Release, *Lowe's Introduces LoweBot - The Next Generation Robot to Enhance the Home Improvement Shopping Experience in the Bay Area*, PR NEWSWIRE (Aug. 30, 2016), available at <http://www.prnewswire.com/news-releases/lowes-introduces-lowebot--the-next-generation-robot-to-enhance-the-home-improvement-shopping-experience-in-the-bay-area-300319497.html> (discussing Lowe's new robot that can assist employees and customers by, for example, helping them locate products in the store); 9. Denise Johnson, *The Impact of Robots Replacing Humans in the Workplace*, CARRIER MANAGEMENT (Aug. 27, 2015), available at <http://www.carriermanagement.com/features/2015/08/27/144510.htm>; 10. 29 U.S.C. § 201 et seq. 11. *Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1206 (2011).



by eliminating the obligation to compensate employees for down-time formerly spent at the workplace. However, under current employment laws, like the California Labor Code, on-call time may still be compensable depending on the amount of control the employer exerts over the employee's ability to engage in personal activities.<sup>12</sup>

### **Workplace Displacement**

The main concern for most individuals in the workforce is the potential displacement of jobs by robots and automation. While employers are not prohibited from redesigning their workforce to eliminate human jobs, employers should plan for and take appropriate steps to ensure a smooth transition. For example, where human jobs have been eliminated, employers could provide severance agreements in exchange for releases from employees who are affected by a reduction in force (RIF) or retrain employees for alternative positions within the company. For employers with more than 100 employees, replacing the workforce with robots may trigger legal obligations under the Worker Adjustment and Retraining Notification Act (WARN Act).<sup>13</sup> Under the WARN Act, certain employers may be required to provide 60 days' advance notice to employees, union representatives, and state and local government officials if they decide to (1) close a plant that would result in a loss of 50 or more employees during a 30-day period; or (2) institute a mass layoff at a site that would result in a loss of 500 or more employees (or in the case of 50 to 499 employees, if 33% of the active workforce is affected). In addition, some states, such as California, have a state WARN Act with which an employer may have to comply.<sup>14</sup>

### **Discrimination**

Mass layoffs may also have an unintended consequence on a protected group of individuals. Courts recognize two separate theories of discrimination in the workplace: disparate treatment and disparate impact. The traditional understanding of discrimination that is familiar to most lay persons is the disparate treatment theory, where an employer intentionally discriminates against an employee on the basis of a protected characteristic, such as the employee's race, sexual orientation, gender, disability, age, religion, etc. However, even when an employer has no discriminatory animus, there is a danger that the policies, practices, rules, or other systems used in a RIF may appear innocuous or neutral on their face, but result in a disproportionate impact on a protected group. A reduction in force that disproportionately impacts a protected group, such as older workers or women—two groups that have historically been underrepresented in the technology and engineering field—may lead to disparate impact discrimination claims on either individual or class action bases.

### **Accommodations for Employees with Disabilities**

Under the Americans with Disabilities Act,<sup>15</sup> employers are required to provide reasonable accommodations to qualified employees with disabilities.<sup>16</sup> Generally, this means providing an accommodation that does not cause an undue hardship to the employer's operations.<sup>17</sup> With the introduction of advanced robotic systems and related technologies, there may be a significant increase in the number and types of jobs that persons with disabilities will be able to perform. In addition, we are likely to see the idea of what accommodations are

<sup>12</sup> Mendiola v. CPS Security Solutions, Inc., 60 Cal. 4th 833, 840 (2015). <sup>13</sup> 29 U.S.C. § 2101 et seq. <sup>14</sup> See, e.g., California Worker Adjustment and Retraining Notification Act, CAL. LAB. CODE § 1400 et seq. <sup>15</sup> 42 U.S.C. § 12101 et seq. <sup>16</sup> 42 U.S.C. § 12112 et seq. <sup>17</sup> 42 U.S.C. § 12112 et seq.



## Related Content

For an explanation on which employers must comply with the Fair Labor Standards Act, which employees are covered by the law, and the most common exclusions from coverage, see

### > [WHICH EMPLOYERS MUST COMPLY WITH THE FLSA AND WHICH WORKERS ARE COVERED?](#)



**RESEARCH PATH:** [Labor & Employment > Wage and Hour > FLSA Requirements and Exemptions > Practice](#)

[Notes](#)

For a discussion on the steps an employer should take when implementing a reduction in force and to comply with the federal Worker Adjustment and Retraining Notification Act (WARN), see

### > [IMPLEMENTING A REDUCTION IN FORCE AND COMPLYING WITH WARN](#)



**RESEARCH PATH:** [Labor & Employment > Investigations, Discipline, and Terminations >](#)

[Discharge and Layoffs/RIFs > Practice Notes](#)

For more information on disparate treatment and disparate impact discrimination claims, see

### > [UNDERSTANDING DISPARATE TREATMENT](#)



**RESEARCH PATH:** [Labor & Employment > Discrimination and Retaliation > EEO Laws and](#)

[Protections > Practice Notes](#)

### > [NAVIGATING DISPARATE IMPACT CLAIMS](#)



**RESEARCH PATH:** [Labor & Employment > Discrimination and Retaliation > EEO Laws and](#)

[Protections > Practice Notes](#)

reasonable evolve over time. Robotics and automation will probably become more affordable as they become the norm, thus expanding the reasonable accommodation options for employees and making some undue hardship defenses less viable for employers. For example, in the foreseeable future, it may be a reasonable accommodation for an employer to provide employees who are confined to a wheelchair or have lifting restrictions with exoskeletons that will assist them with performing manual operations. Thus, an employer's obligation to engage in an interactive discussion may include

the consideration of expanded accommodation options inspired by creative new technologies.

## Health and Safety

The federal Occupational Safety & Health Act (OSHA),<sup>18</sup> as well as some equivalent state statutes—such as the California Occupational Safety and Health Act of 1973<sup>19</sup>—dictate health and safety standards for workplaces. Currently, OSHA does not have any standards that specifically target robotics and automation in the workplace.<sup>20</sup> One concern is that workers performing their jobs alongside robotic systems could be injured by the system itself or by human error. Whereas heavy robots used to typically do their work within a safety cage, companies are more commonly using collaborative, light-weight robots that work alongside their human counterparts. Such proximity may increase the physical interaction between workers and machines.<sup>21</sup> As companies incorporate these technologies, they should ensure appropriate safety mechanisms and training programs are in place, including presence or proximity detectors that halt all robotic motion when they detect the presence of body parts or other objects in close proximity to the robot or to moving or otherwise hazardous parts. Additionally, experts actually report a positive impact on safety due to robotics—the increase in automation has actually led to the fall of workplace fatality rates.<sup>22</sup> Robots and automation may also be used to protect workers from repetitive stress injuries or to improve ergonomics.

## Practical Tips for Employers

Robotic technology, which was once just the stuff of science fiction, is closer to reality than many people may realize. Recent booms in development, such as improvements in cloud computing, sensor technology, and data analytics, coupled with falling prices, have led to exponential growth in robotics, automation, and artificial intelligence. Employers in all industries should start planning now.

## Human Resources and Legal Impact


As companies incorporate robotics and automation into their labor pools, they should involve their human resources and legal departments to consider potential areas of risk or liability. Human resource and legal professionals can help strategize how to overcome potential workplace issues and implement policies and procedures to reduce risk. Companies at the forefront of this new technological revolution may also consider working to shape the development of legislation and related regulations.

18. 29 U.S.C. § 651 et seq. 19. Cal. Lab. Code § 6300 et seq. 20. However, note that OSHA did issue such guidelines in 1987, which are now vastly outdated. See OSHA, *Guidelines for Robotics Safety*, Instruction Pub. No. STD 01-12-002 (PUB 8-1.3), (Sept. 21, 1987) ("OSHA Guidelines"), available at [https://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=DIRECTIVES&p\\_id=1703](https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=DIRECTIVES&p_id=1703). In addition, Section IV: Chapter 4 of OSHA's Technical Manual also addresses Industrial Robots and Robot System Safety (available at [https://www.osha.gov/dts/osta/otm/otm\\_iv/otm\\_iv\\_4.html](https://www.osha.gov/dts/osta/otm/otm_iv/otm_iv_4.html)) and OSHA's Concepts and Techniques of Machine Safeguarding. OSHA 3067 (1992) (Revised) contains a chapter on Robotics in the Workplace (available at [https://www.osha.gov/Publications/Mach\\_SafeGuard/toc.html](https://www.osha.gov/Publications/Mach_SafeGuard/toc.html)). 21. OSHA Guidelines, *supra* n.20, at App. A, sec. A-5. 22. OSHA Guidelines, *supra* n.20, at App. A, sec. A-2.

## Related Content


For a detailed overview of the Americans with Disabilities Act and its requirement to provide reasonable accommodations to qualified employees with disabilities, see

> [AMERICANS WITH DISABILITIES ACT: NAVIGATING EMPLOYER REQUIREMENTS AND MAKING REASONABLE ACCOMMODATIONS](#)

 **RESEARCH PATH:** [Labor & Employment > Attendance, Leaves, and Disabilities > The ADA and Disability Management > Practice Notes](#)


For guidance on complying with Occupational Safety and Health Act, see

> [NAVIGATING OSH ACT REQUIREMENTS, INSPECTIONS, CITATIONS, AND DEFENSES](#)

 **RESEARCH PATH:** [Labor & Employment > Workplace Safety and Health > Occupational Safety and Health Act > Practice Notes](#)

## Training and Workforce Displacement

Employers should also consider taking proactive steps to plan for potential workforce displacement events. For example, employers may develop training programs to help workers develop complementary skills and knowledge or move into different roles that are not being automated.

Despite the unique workplace issues created by technological advancements, employers who are proactive will likely see positive impacts on their business as a result of robotics and related technologies. 

---

**Karen Y. Cho** represents management in all types of employment disputes at Morgan, Lewis & Bockius LLP in San Francisco. She defends and counsels employers including wage and hour class actions; Private Attorneys General Act representative actions; and single or multi-plaintiff discrimination, harassment, wrongful termination, and breach of contract disputes. She may be reached at [karen.cho@morganlewis.com](mailto:karen.cho@morganlewis.com).

---

 **RESEARCH PATH:** [Labor and Employment > Privacy, Technology and Social Media > Policies and Procedures > Articles](#)



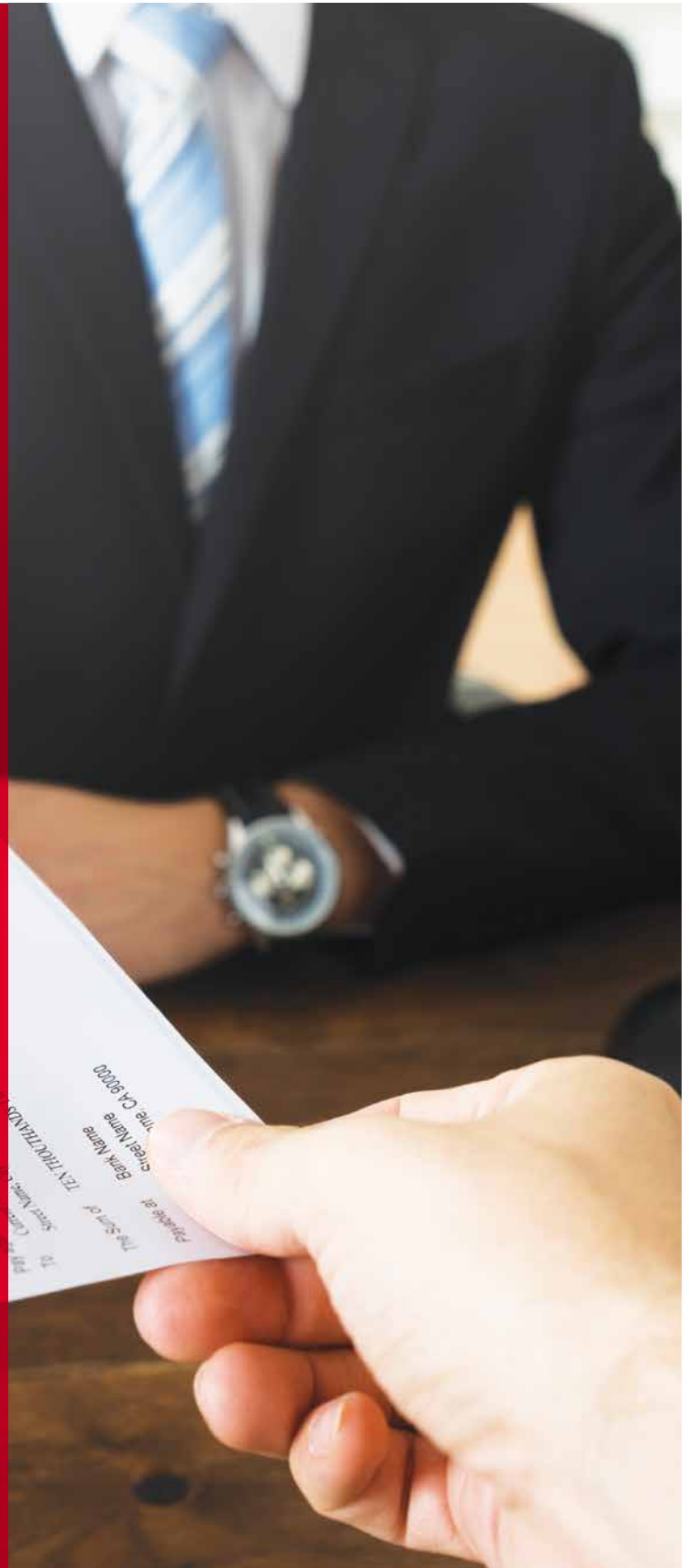


LexisNexis®

Lexis Practice Advisor®

# START HERE TO GET IT RIGHT

Practical guidance clarifies all facets of employee benefits and executive compensation to help you complete your work effectively and efficiently. Includes access to Transactions Search powered by Intelligize®, so you can glean insights into the latest trends from publicly filed contracts to support your drafting.



*Lexis Practice Advisor® Employee  
Benefits & Executive Compensation*

[LEXISNEXIS.COM/PRACTICE-ADVISOR](https://www.lexisnexis.com/practice-advisor)

800.628.3612

40+

PRACTICE AREA EXPERT  
ATTORNEY AUTHORS



GUIDANCE LINKED  
TO DEEPER RESEARCH

100+

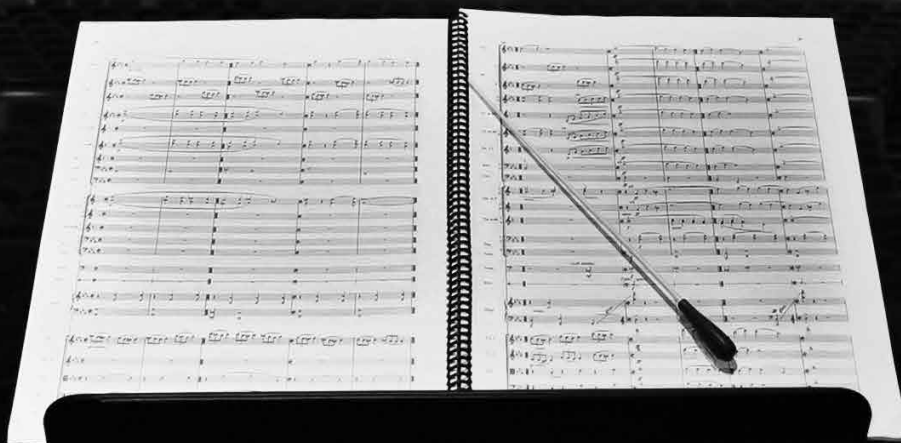
ANNOTATED  
FORM & CLAUSES





Holly K. Towle

# IN-HOUSE COUNSEL'S ROLE **IN CYBERSECURITY & DATA PROTECTION**



This article concerns the question, “What is the role of internal counsel in cybersecurity?” The answer is easier stated than accomplished, but it is essentially this: The role of internal counsel is to use internal and external resources to become knowledgeable conductors of the data security symphony their company must play for regulators, customers, vendors, and competitors.

#### THE CONDUCTOR CANNOT HOPE TO KNOW EVERYTHING

about each section of the orchestra, (e.g., what strings, woodwinds, brass, and percussion must do in order to play their part). However, each section (and subsection) has its own chair who can determine that with the help of internal or external advisors. The role of the conductor is to coordinate and adjust the entire orchestra to create a compliant and harmonious overall data security performance, determining and managing interpretation, balance, tempo, and phrasing.

In reality, this analogy is helpful, but false. In an orchestra, every musician has the composer's entire score sitting on his or her music stand, all marked up and ready to be played. There is no one composer of the legal score for a data security performance. The company must compose its own score based on laws, standards, and guidance that are, simultaneously, vague, too broadly written to follow, written in overwhelming detail, filled with dissonant notes, and variable locally, nationally, and internationally. This makes the score arduous and expensive to compose and learn and, as any hacker knows, perfection is not possible.

Hence the role of the conductor. A conductor who can glean—directly or indirectly through section chairs—the business, data flows, and laws governing each of the sections making up the company's orchestra has the best chance of creating the most compliant data security symphony.

The following questions are intended to help internal counsel as conductor or section chairs compose and orchestrate the data security music their company must play.

#### What Law and Standards Apply to Each Section, Movement, or the Overall Symphony?

Unlike composers, legislatures and regulators tend to dictate in very broad strokes how data security must operate because one size will not fit all. What works today might not work tomorrow. A data security symphony is more like a greatest hits evening (i.e., a hodgepodge of content that must be cobbled together based on a company's particular circumstances). U.S. data security laws are made up of non-uniform federal, state, and local requirements that vary by industry sector (e.g., financial, energy, telecom, retail etc.); activity (e.g., using credit reports, accepting commercial or consumer payments, using big data algorithms etc.); data type (e.g., health,

financial, biometric, geo-location, children's etc.); data device (e.g., Internet of Things device, augmented reality device, wearables etc.); and so on.<sup>1</sup>

Internal or external legal counsel and consultants can help companies deal with the above locally, nationally, and internationally, but there is no global solution and the initial work will need to be updated as laws, administrations, and data security threats change. The scope and complexity of this endeavor is obvious and procrastination can be particularly deadly. Experience a data security breach triggering laws in almost all states and an increasing number of foreign countries, receive a ransomware threat for company data that was not appropriately backed up, or discover that company crown jewels such as intellectual property, trade secrets, or business documents have been hacked, and any procrastination can result in a crushing reality with long term consequences (such as 20-year regulatory orders).



<sup>1</sup> See generally Towle, *The Law of Electronic Commercial Transactions*, <https://store.lexisnexis.com/categories/product/the-law-of-electronic-commercial-transactions-skuusku-us-F53>, at Chapter 6 (Attribution: Identifying the Parties), Chapter 10 (Liability for Informational Content), Chapter 12 (Privacy and Data Protection), Chapter 15 (Identity Theft), and Chapter 16 (Data Security) etc.



COMPANIES GOVERNED BY SECTOR SPECIFIC LAWS, SUCH AS MEMBERS OF THE BANKING, SECURITIES, INSURANCE, ENERGY, TELECOM, AND HEALTHCARE SECTORS, MAY WISH TO START BY DEALING WITH THEIR FEDERAL AND STATE SECTOR-SPECIFIC LAWS.

#### Examples of Selected, General Starting Points

- **General.** With respect to generic data security programs, the National Institute of Standards and Technology (NIST) provides a federal framework for reasonable security<sup>2</sup> that many companies like to use—if only by analogy. However, the Federal Trade Commission (FTC) has warned that the NIST Framework is not a cure-all, at least for companies subject to FTC jurisdiction.<sup>3</sup> For those companies, FTC staff has prepared a general guide about FTC enforcement orders and has begun a blog to give businesses
- a heads-up about what the FTC views as unreasonable security.<sup>4</sup> For companies tempted to ignore these orders and guidance as not relevant because they are not actual law or regulation, note that, legally or not, the FTC has spent over a decade creating its privacy and data security regime just that way.<sup>5</sup>
- **State.** Some state laws essentially require reasonable data security while others are very specific, such as New York rules for financial institutions. Some of the wording should not be taken at face value, (i.e., often there will purport to be hidden mandates such as in California).<sup>6</sup>
- **Sector specific.** Companies governed by sector-specific laws, such as members of the banking, securities, insurance, energy, telecom, and healthcare sectors, may wish to start by dealing with their federal and state sector-specific laws. Although sector is usually a reference to an industry sector, each sector of activities, data, or devices, etc. can also have starting points (such as FTC guidance on security for connected items in the Internet of Things).<sup>7</sup>

2. See NIST Cybersecurity Framework (<https://www.nist.gov/cyberframework>). See also NIST Baldrige Cybersecurity Excellence Builder (<https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf>), a self-assessment tool which is intended to blend two widely used NIST resources: the organizational performance evaluation strategies from the Baldrige Performance Excellence Program (<https://www.nist.gov/baldrige>) and the risk management mechanisms of the NIST Cybersecurity Framework. For more information about FTC requirements as indicated in its enforcement actions and a new blog, see Endnote 5. 3. The FTC has noted this question (emphasis added): "If I comply with the NIST Cybersecurity Framework, am I complying with what the FTC requires?" The FTC was not willing to answer "Yes," although it did admit that the Framework is consistent with the FTC's approach: With that bit of background on the FTC's data security program, let's get back to the question, "If I comply with the Framework, am I complying with what the FTC requires?" **The Framework is not, and isn't intended to be, a standard or checklist.** It's meant to be used by an organization to determine its current cybersecurity capabilities, set individual goals, and establish a plan for improving and maintaining a cybersecurity program, but it doesn't include specific requirements or elements. In this respect, there's really no such thing as "complying with the Framework." **Instead, it's important to remember that the Framework is about risk assessment and mitigation. In this regard, the Framework and the FTC's approach are fully consistent:** The types of things the Framework calls for organizations to evaluate are the types of things the FTC has been evaluating for years in its Section 5 enforcement to determine whether a company's data security and its processes are reasonable. By identifying different risk management practices and defining different levels of implementation, the NIST Framework takes a similar approach to the FTC's long-standing Section 5 enforcement. See [https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc?utm\\_source=govdelivery](https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc?utm_source=govdelivery). 4. See "Start with Security: A Guide for Businesses" (<https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>) and "Stick with Security" ([https://www.ftc.gov/news-events/blogs/business-blog/2017/07/stick-security-insights-ftc-investigations?utm\\_source=govdelivery](https://www.ftc.gov/news-events/blogs/business-blog/2017/07/stick-security-insights-ftc-investigations?utm_source=govdelivery)). 5. Strong arguments can be made that the FTC has exceeded and is exceeding its legal authority, but it has had some initial success in litigation regarding that issue, and it is expensive and risky to litigate against a regulator with the power to impose material penalties. Some companies take a two-pronged approach—heeding FTC warnings just in case it is proceeding legally, but also supporting efforts to require the FTC to heed applicable law. See for example, Chapter 12.16[3], Towle, *The Law of Electronic Commercial Transactions*, <https://store.lexisnexis.com/categories/product/the-law-of-electronic-commercial-transactions-skusku-us-F53>. 6. See *Cal. Civ. Code Sec. 1798.81.5 (b)*. Using defined terms, it literally creates a very general obligation: (b) A business that owns or licenses or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. However, hidden in a report by the California Attorney General on data breaches, the California Attorney General purported to interpret it as including 20 very detailed and material controls. See "California Data Breach Report February 2016" (<https://oag.ca.gov/breachreport2016>, emphasis added) (stating that the statute requiring businesses to use "reasonable security" is a set of controls from an industry standard. The following statement is made in the "Recommendations" section of the Executive Summary: "The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security." 7. See for example, the FTC's "Careful Connections, Building Things in the Internet of Things" (<https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf>) (2015) and Footnote 9.



## What Topic or Data Specific Rules Apply?

Reasonable data security goes beyond protection of obvious data such as crown jewels and personal information. It also extends to arcane and new activities and devices. For example:

- Employers who directly credit employee paychecks to their bank accounts are governed by payment system rules privately published by the National Automated Clearing House Association (NACHA),<sup>8</sup> and those rules have data security requirements and data breach notice guidance.
- Manufacturers, retailers, service providers, and other companies involved in the Internet of Things (e.g., smart televisions), will not only need to be designed with security in mind<sup>9</sup> but also pursuant to device-specific laws going beyond security.<sup>10</sup>
- Companies using biometric data need to locate and comply with laws defining and concerning such data. The fact that security might be improved with biometric data such as an iris scan does not decrease compliance obligations—to the contrary, solutions involving sensitive data tend to increase them.<sup>11</sup>

## What about Third Parties and Contracts?

Governmental laws or guidance applicable to your company set the beat for data security music but contracts will impact it. Internal counsel should create (or cause to be created) an offensive and defensive contracting strategy for employees, service providers, suppliers, and essentially anyone else with access (physical or electronic) to company premises, systems, data, or other information. This largely is not optional. For example, the California law noted above that requires businesses to have reasonable data security also requires the businesses to trickle down-up-or-over that obligation to third parties via contract.<sup>12</sup>

### Practice Tips

- **Review the contract to see if it supports the sales pitch.** Even if the company hires a third party precisely because that party holds itself out as being able to provide security for a complex area (e.g., third-party token provider for a retailer trying to comply with payment industry rules), the contract actually offered to the company often will not stand behind the touted solution or even the third party's Payment Card Industry (PCI) compliance

role. The practice tip is to read and renegotiate the contract, or attempt to find another provider.

Social network contracts<sup>13</sup> provide another example. Assume internal counsel's company provides an app, website, or Internet of Things device that collects personal information from children. The company likely knows about the need for compliance with [Children's Online Privacy Protection Act](#) or similar state laws,<sup>14</sup> but might assume that social network or data analytic companies that collect data for a living will take care of their own compliance. Often that is not the case, however. More typically, the social network or data analytic contract allocates compliance to the company or might require the company to take particular steps. The practice tip is the same as above, but with an additional tip: work with the IT section so that it will seek legal review of the social network and analytics contracts before third-party technology is allowed to take or receive data.

- **Be skeptical of the actual wording in otherwise required contracts.** When the company is on the receiving end of a third party's data security clause, don't believe the argument that the law requires the third party's wording. The law might require a contract, but not the particular wording or risk allocation. For example, the federal [Gramm-Leach-Bliley Act](#) (GLBA) requires financial institutions (FI) to have GLBA security, but a contract requiring the company "to comply with the GLBA" is a trap. Each FI must create a very detailed, custom security program for itself, and the company cannot know what that custom program actually requires. The company might be able to comply with a reviewable rider narrowly setting forth exactly what the FI needs the company to do, however.
- **Fill out the Data Security Breach Response Plan appendices.** Read and work the data security contractual obligations into the company's Data Security Breach Response Plan before a breach can occur. For example, if a credit card data breach occurs and the company grabs its Data Security Breach Response Plan, will the appendix for "payment card breaches" still be empty or will it be fully fleshed out with the exact reporting requirements and deadlines? If it's still empty, it's almost a certainty that by the time the company or its counsel reads through the myriad rules and policies (which are changing at ever-shortening intervals), it will have missed a deadline and be exposed to higher penalties.

8. See <https://www.nacha.org/rules>. 9. See for example, NIST Special Publication 800-160 advising those involved with developing Internet-connected systems and devices to build security safeguards directly into their products and then to consider security at every lifecycle stage (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf>). See also FTC Staff Report Internet of Things: Privacy & Security in a Connected World, 7-10 (Jan. 2015), (<https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>), and an illustrative FTC enforcement action, *FTC v. D-Link Corporation et al.*, FTC Matter/File Number: 132 3157 (alleging D-Link failed to take reasonable steps to secure its routers and Internet Protocol cameras, potentially compromising sensitive consumer information). 10. See Chapter 12.23 (discussing California law mandating particular contract formation rules for televisions with voice recognition features) and Chapter 10.14 (consumer Internet of Things issues) of Towle, *The Law of Electronic Commercial Transactions*, <https://store.lexisnexis.com/categories/product/the-law-of-electronic-commercial-transactions-skuusSku-us-F53>. 11. For an example of a biometric statute, see Illinois Biometric Information Privacy Act (BIPA), 740 Ill. Comp.Stat. Ann. 14/1, et seq. (the introduction to this act says: "The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information"). 12. See for example, *Cal. Civ. Code Sec. 1798.81.5 (c)*: (c) A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not subject to subdivision (b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Several FTC enforcement orders also require contracts, including with remote parties. 13. For discussion of what these contracts are and where they can be found, see Chapter 10.14[1] Towle, *The Law of Electronic Commercial Transactions*, <https://store.lexisnexis.com/categories/product/the-law-of-electronic-commercial-transactions-skuusSku-us-F53>. 14. For a discussion of this topic, see Chapter 12.11 (Children's Online Privacy Protection Act and State Statutes Regarding Children or Other Minors) of Towle, *The Law of Electronic Commercial Transactions*, <https://store.lexisnexis.com/categories/product/the-law-of-electronic-commercial-transactions-skuusSku-us-F53>.



This will be so even if the company is working closely with its merchant bank representative (including one who fails to mention which brands are outside the scope of what the representative is doing).

### How Do Company Policies Mesh with Its Actual Security Program

In 2014 the Heartbleed virus essentially invalidated Secure Sockets Layer (SSL) as a reasonable encryption method and by 2015, the Payment Card Industry Data Security Standard (PCI DSS) warned against its use.<sup>15</sup> Yet today in 2017, it still is rather common to see a website privacy policy touting the security of SSL encryption.<sup>16</sup> If the

IT section stopped using SSL but forgot to tell the section charged with amending the privacy policy, that lack of coordination can create dissonance in the compliance music.

Another example is the IT group that creates security for company emails accessed by employee-owned smartphones by implementing a kill-switch solution allowing the company to wipe all content if the phone is stolen or lost. Many companies have that solution, but how many IT departments worked with their legal departments to back it with an appropriate contract between the company and employee?

A successful conductor needs to be in a position to learn what each section of its data security orchestra is actually doing so that needed harmonization can be created.

<sup>15</sup>. By analogy, see for example, PCI DSS, version 3.1 (removed from examples of acceptable encryption, SSL and early Transport Layer Security (TLS)). The current version of PCI DSS, version 3.2 required service providers to provide a secure offering by June 2016 and assumes that all entities will cease use of SSL and TLS 1.0 as a security control by June 30, 2018. An industry blog says this: "Despite the 2018 deadline, you should move to replace these protocols as quickly as possible. Of the top 10 critical vulnerabilities identified through penetration testing by Trustwave in 2015, SSL protocol vulnerabilities ranked first." Trustwave blog 4/18/16 at [https://www.trustwave.com/Resources/Trustwave-Blog/What-You-Need-to-Know-About-PCI-DSS-3-2-\(and-Why-Security-Comes-First\)/?mkt\\_tok=eyJpIjoiWldOaU1XVmxZVGcwTnpVMilsInQiOiIwQ01zNHBMWVNWckNWZEtKROVcLzJlaTRaYW93ejlmdU5xZFJGMGNmUFBtbytEeUloaDR6MkpXNTRMVG9ibV5WDdcL3lrZ0N1UjUoTTJ4ZHNiZ2ZlL1VZWGtOeFFibUhPYXR6bkVncFRmVmpSMD0ifQ%3D%3D](https://www.trustwave.com/Resources/Trustwave-Blog/What-You-Need-to-Know-About-PCI-DSS-3-2-(and-Why-Security-Comes-First)/?mkt_tok=eyJpIjoiWldOaU1XVmxZVGcwTnpVMilsInQiOiIwQ01zNHBMWVNWckNWZEtKROVcLzJlaTRaYW93ejlmdU5xZFJGMGNmUFBtbytEeUloaDR6MkpXNTRMVG9ibV5WDdcL3lrZ0N1UjUoTTJ4ZHNiZ2ZlL1VZWGtOeFFibUhPYXR6bkVncFRmVmpSMD0ifQ%3D%3D). <sup>16</sup>. A random search in 2017 revealed this example in a privacy policy: "The security of your personal information is of the utmost importance to [X]. [X] only transmits personal information, including sensitive information (such as credit cards), using secure sockets layer technology (SSL)."

**PARTIAL VICTORY CAN BE DECLARED  
WHEN A DATA SECURITY PROGRAM  
IS DEVELOPED AND FINISHED BASED  
ON APPROPRIATE BACKGROUND AND  
COMPLIANCE WORK.**

### What Documentation is Advisable?

Documentation of a company's data security program can buttress its data security efforts even when not literally required. Lack of documentation is taken by some regulators as a warning signal that the company is not serious about data security.

#### Practice Tips

Attempt to:

- Create required or otherwise reasonable documentation that is relevant to the company's legal and business circumstances.
- Avoid over-promising. For example, in a Data Security Breach Response plan, why say that the core planning group "must" adhere to the plan so as to "ensure" "full" compliance with applicable laws? Few breaches will allow the group to meet those mandates. A more realistic approach, when legally possible, would be to require the group to make reasonable efforts to meet the plan in light of the urgent, ambiguous, legal, and technological circumstances of the particular data emergency at issue, and allow the group to make good faith judgments.

### What about Acquisitions?

Whether a company wants to acquire other companies or be acquired, data security is an issue. Poor data security can decrease the purchase price and increase indemnities and holdbacks if your company is being acquired. If your company is the acquirer, development of due diligence checklists to deal with the range of data security issues (as well as the raft of other new due diligence issues created by our digital economy) is a must in order to understand what risks the acquirer may be buying. Typical M&A checklists often do not deal with this topic at all or appropriately.

In 2011, the U.S. Securities and Exchange Commission (SEC) issued guidance regarding disclosure obligations of publicly traded companies relating to cybersecurity risks and cyber incidents.<sup>17</sup> As explained by the SEC, "material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of

#### Related Content

For detailed information on the steps to take before and during a data breach, see

> **PLANNING FOR & MANAGING A DATA BREACH**



**RESEARCH PATH:** [Corporate Counsel >](#)

[Cybersecurity > Planning for and Managing a Data Breach > Practice Notes](#)

For assistance in drafting a data breach notification letter, see

> **PREPARING A BREACH NOTIFICATION LETTER**



**RESEARCH PATH:** [Corporate Counsel >](#)

[Cybersecurity > Planning for and Managing a Data Breach > Practice Notes](#)

For a discussion on the key issues to consider when drafting or reviewing a company's data privacy policy, see

> **DRAFTING PRIVACY POLICIES**



**RESEARCH PATH:** [Corporate Counsel > Policies and Procedures > Privacy, Security and HIPAA > Practice](#)

[Notes](#)

For guidance on creating a plan to assign priorities and responsibilities for cybersecurity within an organization, see

> **CYBERSECURITY RESILIENCE IMPLEMENTATION PLAN**



**RESEARCH PATH:** [Corporate Counsel >](#)

[Cybersecurity > Information Security > Forms](#)

the circumstances under which they are made, not misleading." The SEC guidance officially brought certain security risks into the realm of SEC-required disclosures. Similar issues exist for non-reporting companies and the SEC materials can be helpful, if only by analogy, when creating a data security program.

To illustrate, does the company's standard due diligence checklist ask about what material data security incidents the target has experienced but did not disclose to data subjects or regulators, and could that nondisclosure create a reportable issue for a public company? Regardless of reporting rules, does that nondisclosure create another risk the acquirer needs to consider before proceeding with the deal? In recent years, the SEC has been buttressing its guidance and data security expectations with data security questionnaires and examination signals that can be worked into

<sup>17</sup> See Disclosure Guidance: Topic No. 2, Cybersecurity, Div. of Corp. Finance SEC (10/13/11) (guidance re disclosure obligations relating to cybersecurity risks and cyber incidents) (<http://www.sec.gov/divisions/corpfm/guidance/cfguidance-topic2.htm>).



any due diligence checklist. Of course, that will not be the end of the checklist.

### When Can Internal Counsel Declare Victory?

Partial victory can be declared when a data security program is developed and finished based on appropriate background and compliance work. Unfortunately, final victory can never be declared. Data security requirements are ambiguous in the first place and ever-evolving.

Non-privacy/security lawyers correctly laugh at the thought of a regulator purporting to use anything other than formal law or regulations to define existing or future legal obligations of companies, but the reality is not funny. Legal or not, that is how many regulators are regulating and the jury is still out on whether and the extent to which that approach is legal. In the meantime, it is the regulator that gets to decide whether to bring an enforcement action.

### Conclusion

Data security is not a single piece of music. It is a symphony—a large, multi-movement work involving all sections and subsections of the orchestra and maneuvering through a full range of interpretation,

balance, tempo, and phrasing that must change as laws and technology change. Unlike a real symphony, the data security symphony each company must play has not already been written. Each company must compose its own version based on applicable laws relevant to its particular venues, industry, activities, products, data, or other information. The role of the company's internal counsel can be to conduct the entire orchestra and chair the various sections. **L**

---

**Holly K. Towle** is the author of [The Law of Electronic Commercial Transactions](#), an information-rich treatise regarding digital economy legal issues about which she speaks and consults. Before her recent retirement, Ms. Towle spent her career as a partner with K&L Gates LLP, an international law firm, where she focused on electronic business issues, including data privacy and security, big data, artificial intelligence, consumer protection and payment system compliance, e-contracting structures, and legal distinctions between information and goods or services.

---



**RESEARCH PATH :** [Corporate Counsel](#) > [Cybersecurity](#) > [Planning for and Managing a Data Breach](#) > [Articles](#)





Stephen E. Reynolds and Nicole R. Woods ICE MILLER LLP

# What Companies Need to Know about **Protecting Confidential Information under the New ACC Guidelines**

In response to the increased concern surrounding cybersecurity, the Association of Corporate Counsel (ACC) has released the Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information. The authors of this article discuss the guidelines, which can serve as a benchmark for law firm cybersecurity practices.

**MORE AND MORE FREQUENTLY, HEADLINES ARE FILLED** with news of crippling cyberattacks designed to cause the most chaos in the shortest amount of time. Recent examples include the WannaCry and Petya ransomware attacks that affected businesses worldwide, including many law firms. The WannaCry attack affected more than 230,000 computers in more than 150 countries within a single day, causing massive disruptions.

According to the [2016 ABA TECHREPORT](#), 20%–25% of law firms have already experienced a data breach. In fact, one large law firm, which recently touted its cybersecurity expertise, was hit by the Petya attack and suffered several days of total system shutdown. It is no surprise, therefore, that two-thirds of chief legal officers and general counsels rank information privacy and protection of corporate data as “very” or “extremely” important.



In response to the increased concern surrounding cybersecurity, the ACC released the Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information.<sup>1</sup> The ACC hopes these guidelines will serve as a benchmark for law firm cybersecurity practices.

<sup>1</sup> ACC Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information, available at <http://www.acc.com/advocacy/loader.cfm?csModule=security/getfile&pageid=1454057&page=/legalresources/resource.cfm&qstring=show=1454057&fromLibrary=1&title=Model%20Information%20Protection%20and%20Security%20Controls%20for%20Outside%20Counsel%20Possessing%20Company%20Confidential%20Information%20&recorded=1>.

## Are These Guidelines the New Standard for Outside Counsel?

Although the ACC intends for the guidelines to “offer in-house counsel a stream-lined and consistent approach to setting expectations with respect to the data security practice” of outside counsel, the ACC repeatedly cautions that the guidelines should not serve as an industry standard. It specifically provides that the guidelines are not intended to “substitute for corporate counsel’s own legal analysis and good judgment,” and they are “not intended to establish any industry standards for any purpose for either the company client or outside vendor.”

Although ACC goes out of its way to hopefully avoid setting minimum standards, the guidelines themselves read like a contract, requiring that outside counsel “shall” complete certain tasks and meet certain standards.

## What Do the Guidelines Suggest?

The guidelines set out a framework of various requirements in the hopes that outside counsel will ensure appropriate

technical and organizational measures for protection of the client’s company confidential information and other similar data. Confidential information is broadly defined and includes items such as employee personally identifiable information, information relating to the company’s physical or cybersecurity measures, material nonpublic information (for publicly traded companies), and protected health information.

Outside counsel may already satisfy some of the more routine guidelines as part of their current operating procedures. For example, outside counsel must return or destroy company confidential information at the conclusion of the engagement unless required to maintain the information by law. Outside counsel must also continually monitor networks, employees, and subcontractors for malicious activity or activity that may damage the company’s confidential information. Additionally, they must perform assessments on their systems to minimize security vulnerabilities. Law firms likely already have some sort of system or policy in place to satisfy these requirements or are in a position where they could quickly and easily implement the solutions.





**IN THE EVENT A DATA BREACH DOES OCCUR OR IS SUSPECTED  
TO HAVE OCCURRED, THE GUIDELINES REQUIRE THAT OUTSIDE COUNSEL  
NOTIFY THE COMPANY WITHIN 24 HOURS OF DISCOVERING  
THE ACTUAL OR SUSPECTED BREACH.**

Additionally, outside counsel may already meet the requirement that they install and utilize consistently updated antivirus protection, install routine software patches, and maintain firewalls or other network protections. The guidelines also require outside counsel to have application security and software controls to minimize system and network vulnerabilities. Finally, outside counsel may also already satisfy the requirement that the firm manage access to the company's confidential information, such as limiting access to the information to only certain individuals or certain job functions. Many document management systems provide this functionality, and it is easy to implement.

Two of the guidelines that speak to administrative matters may be either new to outside counsel and/or more burdensome to actualize. First, the guidelines provide that outside counsel will obtain and maintain cyber liability insurance with a minimum coverage level of \$10,000,000. A LogicForce study released in June 2017 stated only 23% of law firms currently carry cybersecurity liability insurance. However, the policies can provide significant benefits, including coverage for damage to data, disruption of business, and reputational harm.

Second, companies may request that outside counsel undertake the process to obtain ISO 27001 certification for its information security management system. This type of certification results from a framework of policies and procedures that include controls for legal, physical, and technical aspects of the system. Obtaining this type of certification can take significant time and can result in significant costs.

The remaining guidelines fall into one of two categories: data handling or physical security.

#### **Data Handling**

When many people think of cybersecurity, they think of encryption. The guidelines are no different. They first focus on encryption in transit. This guideline is uncharacteristically vague. Rather than providing specific encryption requirements, it simply provides that when transferring company confidential information and communicating with the company, outside counsel will use encryption based on guidance provided by the company. This guideline seemingly leaves encryption of

email and other communications up for discussion between the company and outside counsel.

For encryption of data at rest—data not moving through the network—outside counsel must encrypt all company confidential information that resides on any server, computer, or back-up tape. Unlike the guideline for encryption in transit, this guideline specifically requires that counsel use encryption solutions certified against U.S. Federal Information Processing Standard 140-2, Level 2, or an equivalent industry standard. The guidelines also provide the same encryption standard for confidential information that resides on or is transferred to mobile devices, removable media, tablets, and laptops.

In the event a data breach does occur or is suspected to have occurred, the guidelines require that outside counsel notify the company within 24 hours of discovering the actual or suspected breach. After notification, outside counsel must also provide companies with access to an individual who will act as the single point of contact on a 24/7 basis for the company for purposes of addressing the breach.

#### **Physical Security**

Generally speaking, the guidelines require company confidential information to be physically secured against unauthorized access. For law firms that host the confidential information on their own systems and servers, there are many more requirements, and this may be an area where outside law firms fall short of the guidelines.

Outside counsel must implement at least 12 separate physical security precautions, including:

- 24/7 security guards monitoring the entrance to the facility(s) where the confidential information is stored, accessed, processed, or destroyed
- Camera surveillance with active monitoring
- No exterior access points
- Enhanced access to computer rooms such as palm readers, iris recognition, or fingerprint readers

Smaller law firms that host their own data likely do not have these protections currently in place.

## Related Content

For a sample plan setting forth an organization's policies and procedures for maintaining and securing confidential materials, see

### > [WRITTEN INFORMATION SECURITY PLAN](#)



**RESEARCH PATH:** [Corporate Counsel > Policies and Procedures > Privacy, Security and HIPAA > Forms](#)

For more information on cyber liability insurance, see

### > [CYBER-SECURITY INSURANCE](#)



**RESEARCH PATH:** [Corporate Counsel > Business Torts and Insurance > Insurance Policies > Practice Notes](#)

For guidance on negotiating and drafting cloud computing agreements, see

### > [INITIAL CONSIDERATIONS IN CLOUD COMPUTING AGREEMENTS](#)



**RESEARCH PATH:** [Corporate Counsel > Software and Information Technology > Cloud Computing > Practice Notes](#)

For guidance on creating a plan to assign priorities and responsibilities for cybersecurity within an organization, see

### > [CYBERSECURITY RESILIENCE IMPLEMENTATION PLAN](#)



**RESEARCH PATH:** [Corporate Counsel > Cybersecurity > Information Security > Checklists](#)

## How Can Law Firms Implement the Guidelines, and Are There Any Additional Factors to Consider?

Some law firms may already satisfy one or more of the guideline requirements. Others may feel overwhelmed by the seemingly daunting steps they need to take in order to comply. In any case, there are steps firms can take in order to implement the guidelines, as well as additional considerations firms must take into account when formulating their implementation plans.

Firms can add a chief information security officer (CISO) to the payroll. A CISO can be responsible for establishing and maintaining an implementation strategy and is well-versed in the technological aspects of compliance. This allows the attorneys to focus on practicing rather than technical information technology (IT) matters. As part of this, firms may

also consider creating and maintaining a firm-wide and client-wide cybersecurity protocol based on the guidelines. That would eliminate the need, to a large extent, to create individual protocols for each client.

Firms should make sure antivirus software is used and is updated daily for malware definitions. Other security software, such as a firewall, should also be implemented. Firms can also obtain cybersecurity insurance policies, which the American Bar Association began offering in February of this year.

Firms will also need to assess their current system for available encryption methods, including those available for email and other communications. Separate and apart from the ACC guidelines, the ABA has recently provided ethical guidance concerning protection of client communications in Opinion 477R, issued in May 2017.<sup>2</sup>

Previously, the ABA's Opinion 99-413 concluded that use of unencrypted email is a reasonable means to maintain client confidentiality. Opinion 477R, however, now concludes that "it is not always reasonable to rely on the use of unencrypted email." Instead, counsel should make "reasonable efforts to prevent the access or disclosure" of the client's information.

What constitutes "reasonable efforts" on the part of counsel is not a matter of black and white. The Opinion does not provide a toolkit for counsel to utilize in order to ensure proper protection of information. Instead, the Opinion explains that counsel should complete a fact-based analysis in determining what constitutes "reasonable efforts" by considering the factors set forth in Comment [18] to Model Rule 1.6(c). Those factors include, among others, the sensitivity of the information and the likelihood of disclosure. The Opinion specifically states this fact-based analysis "means that particularly strong protective measures, like encryption, are warranted in some circumstances." In addition, the Opinion makes clear that in order to satisfy the duty of competency, attorneys must stay abreast of the benefits and risks of relevant technology.

A firm may choose to simply send sensitive information in an encrypted email when communicating with a client. There are several solutions on the market for both small and large firms to implement such a plan. Some allow the user to choose when to encrypt an email or can automatically encrypt emails if the email or attachments meet specific user-set criteria.

However, even when sending an encrypted email, the metadata of the message—such as sender, recipient, subject line, time, and date—may remain unencrypted and open to prying eyes. In addition, if using a secure web-based email provider such as

<sup>2</sup> ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 477R (2017).



Gmail or Yahoo, the email provider still retains a copy of the entire communication, not just the metadata, and the message will remain vulnerable to possible collection by government or law enforcement. Firms may instead choose to communicate with companies via a secure web portal, which allows for complete protection of the communication from all possible interceptors. All client communications are created and retrieved within the portal, and the entirety of the message, including its metadata, is encrypted. Email is utilized to notify the message recipient that he or she received a new message in the portal, but the message itself is not sent via email. This process is somewhat time-consuming for both the firm and the client, but it is one solution to protect highly sensitive communications.

Finally, in order to address other security measures, law firms that host their own data may consider migrating their information to the cloud, which would place the data in a vendor's data center. Data centers offer both public and private clouds depending on the need of the firm. In both situations, the firm's data is completely segregated. However, with a public cloud, multiple companies share the same set of servers. With a private cloud, the company's data is contained on entirely separate hardware that is not shared. Using a data center can help with the physical security guidelines because it often has the security and supervision the guidelines require.

Cloud computing is relatively new in the legal world, and many firms are hesitant to relinquish control of their data. However, of the 20 states that have reviewed cloud computing from an ethics and confidentiality standpoint, all 20 found that cloud computing is permitted with reasonable care.

In the end, each law firm may choose to conduct its own risk assessment to decide how best to comply with any ethical or client responsibilities for protection of data. **L**

---

**Stephen E. Reynolds**, a former computer programmer and IT analyst, is a partner in Ice Miller LLP's Litigation Group and co-chair of the Data Security and Privacy Practice, focusing his practice on commercial litigation and data security and privacy law.

**Nicole R. Woods** is an associate in the firm's Data Security and Privacy Practice, focusing on complex commercial litigation, including contract disputes, business torts, and financial services litigation. The authors may be reached at [stephen.reynolds@icemiller.com](mailto:stephen.reynolds@icemiller.com) and [nicole.woods@icemiller.com](mailto:nicole.woods@icemiller.com), respectively.

This article was published in the October 2017 issue of Pratt's Privacy & Cybersecurity Law Report. All rights reserved. Visit the website to subscribe.

---



**RESEARCH PATH:** [Corporate Counsel > Compliance, Risk Assessment and Governance > Compliance Programs and Risk Assessment](#)





**Jeffrey Lieberman** SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

# Addressing Retirement Plan Investment Committee Issues

This article identifies best practices to assist a 401(k) plan investment committee in satisfying its fiduciary obligations under the Employee Retirement Income Security Act of 1974 ([29 U.S.C. § 1001, et. seq.](#), as amended) (ERISA). The focus is primarily on steps investment committees can take to monitor plan investment options and service providers.

## Delegation of Authority to Committee

Plan sponsors often use an internal investment committee (the committee) to manage some or all aspects of the ERISA fiduciary responsibilities of an ERISA plan sponsor's board of directors (the board). While the board may delegate responsibility to the plan trustee, a board more commonly delegates the duty of investment and investment service provider selection and monitoring to a committee when such delegation is not prohibited under the governing plan or trust documents.

Typically, the board's delegation to a committee is intended to completely relinquish its ERISA fiduciary responsibilities for the selection and control of plan investments and selected service providers. Alternatively, the board may retain decision-making authority and task the committee to make recommendations to the board. The board would then decide on the ultimate selection or retention issues at hand. This alternative approach is not common, however, when the plan sponsor is a large corporation. If the board wishes, it may delegate to the same or a different committee responsibilities it retains for plan administration.

When the board delegates comprehensive responsibility to a committee, it still retains some fiduciary responsibility as an appointing fiduciary. This is so regardless of whether or not the committee has been identified in governing plan or trust documents as an ERISA named fiduciary. Thus,



the board should request and evaluate periodic committee reports regarding committee actions. The board may require quarterly, semi-annual, or annual reports. Annual reporting is most common.

**REGARDLESS OF THE FIDUCIARIES' INTENT TO APPLY THE  
ERISA SECTION 404(C) SAFE HARBOR, FIDUCIARIES MUST PRUDENTLY SELECT  
PLAN INVESTMENTS AND MONITOR THEIR PERFORMANCE AND THAT OF  
ACCOMPANYING PLAN SERVICE PROVIDERS.**

Also, to delineate the role of the committee and its responsibilities, it is helpful to prepare and have the board or committee adopt a committee charter. Charter responsibilities for an investment committee typically include:

- Establishing, interpreting, and following an investment policy statement for the plan
- Selecting investment options for the plan, including a platform provider
- Establishing an ERISA § 404(c) policy statement (applicable to defined contribution plans with participant-directed investments)
- Selecting a qualified default investment alternative (QDIA) for the plan (applicable to defined contribution plans with participant-directed investments)
- Being responsible for the selection of professional advisers for the plan, including investment managers and consultants, trustees, custodians, and plan auditors –and–
- Regularly monitoring the performance of each investment option and service provider, including the fees charged

**Prudence Standard in Selecting and Monitoring Plan Investments**

A committee with broad powers to select plan investment options falls within ERISA's definition of "fiduciary" through the committee's exercise of authority and control over the plan and plan assets. ERISA § 3(21)(A) ([29 U.S.C. § 1002\(21\)\(A\)](#)). ERISA requires that investment fiduciaries select and monitor plan investments with the care, skill, prudence, and diligence that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims (the prudence standard). ERISA § 404(a)(1) ([29 U.S.C. § 1104\(a\)\(1\)](#)); [29 C.F.R. § 2550.404a-1\(a\)](#). A committee must apply the prudence standard in all of its fiduciary actions. Note that the standard is generally viewed as applying to the decision-making process and not the ultimate results of such decisions (i.e., whether the outcome was right or wrong). This concept of procedural prudence is described more fully in the Lexis Practice Advisor guidance on [Fundamentals of ERISA Fiduciary Duties](#).

*"Appropriate Consideration"*

In fulfilling its duty of prudence, Department of Labor regulations enumerate standards to consider. For example, a plan fiduciary charged with investment duties must give "appropriate consideration" to its investment decisions. [29 C.F.R. § 2550.404a-1\(b\)\(1\)](#). In applying the standard, the fiduciary should (among other items) consider:

- Whether the particular investment or investment course of action is reasonably designed to further the purposes of the plan –and–
- With respect to the plan's asset portfolio:
  - Composition of the portfolio with regard to diversification
  - The liquidity and current return of the portfolio relative to the plan's cash flow requirements –and–
  - The projected return of the portfolio relative to the funding objectives of the plan

The foregoing most clearly apply to a defined benefit plan rather than a defined contribution plan relying on ERISA Section 404(c) protections. But fiduciaries of defined contribution plans, as for defined benefit plans, should consider associated fees in choosing any investment or service provider. A committee for a defined contribution plan thus should consider:

- Relative fees and costs of investment options within the plan
- Risk of loss with respect to any plan investment option –and–
- Historical and projected returns for each investment option

For further discussion regarding application of the "appropriate consideration" standard, see the Department of Labor's guidance on Meeting Your Fiduciary Responsibilities, <https://www.dol.gov/ebsa/publications/fiduciaryresponsibility.html>.

*ERISA Section 404(c) Protections*

Most 401(k) plans or employer-sponsored 403(b) annuity plans provide for participant-directed investments and seek to fall under the ERISA Section 404(c) safe harbor rules. In order

to do so, the plan and its investment menu must satisfy the following conditions:

- Offer a broad range of investment alternatives of varying risk/return profiles in the plan.
  - Generally, this refers to the plan providing at least three funds with diverse risks and returns that, when combined with other potential funds, allow participants the opportunity to minimize the overall risk of loss in their respective portfolios.

- Provide timely notice to participants and beneficiaries of their investment rights, including voting, where applicable, and provide information about the plan investments.

The plan also must provide quarterly account statements to participants and beneficiaries in satisfaction of the plan administrator's ERISA § 105(a)(1)(A) ([29 U.S.C. § 1025\(a\)\(1\)\(A\)](#)) obligations.

- Provide reasonable opportunities to participants and beneficiaries to effect transfers between and among funds.

ERISA § 404(c) ([29 U.S.C. § 1104\(c\)](#)); [29 C.F.R. § 2550.404c-1\(b\)](#).

Regardless of the fiduciaries' intent to apply the ERISA Section 404(c) safe harbor, fiduciaries must prudently select plan investments and monitor their performance and that of accompanying plan service providers. [29 C.F.R. § 2550.404c-1\(d\)\(2\)\(iv\)](#).

### Overview of Investment Option Selection and Monitoring

Foremost of the investment committee's functions is the selection of investment options from which participants and beneficiaries may choose to invest their plan contributions. The committee's selection of the plan's menu of investment options, including employer stock (whether or not identified in the plan document), is itself a fiduciary act and is subject to the prudence standard. Preamble to [29 C.F.R. § 2550.404c-1](#), [57 Fed. Reg. 46906, 46924](#). That standard continues to apply when the committee monitors any of its investment selections to understand whether each investment remains prudent in light of the applicable risks and overall goals of the plan. In monitoring an investment option, the committee should consider changes to the investment option, such as a change to the management team's stated strategy, composition of the management team, fees associated with the investment, or its investment performance over a stated period of time, as well as the investment's role in the plan's investment goals and investment policy statement. Based on this evaluation, the committee should gather sufficient information to determine whether to retain, watch, or eliminate an investment option from the menu.

### Related Content

For a sample board resolution creating an investment or other plan committee, see

#### > [BOARD RESOLUTIONS: RETIREMENT PLAN COMMITTEE APPOINTMENT AND CHARTER ADOPTION](#)



**RESEARCH PATH:** [Employee Benefits & Executive Compensation > Retirement Plans > ERISA and Fiduciary Compliance > Forms](#)

For a discussion of procedural prudence, see

#### > [FUNDAMENTALS OF ERISA FIDUCIARY DUTIES](#)



**RESEARCH PATH:** [Employee Benefits & Executive Compensation > Retirement Plans > ERISA and Fiduciary Compliance > Practice Notes](#)

For more information about ERISA 404(c) notice requirements, see

#### > [KEY ERISA DISCLOSURE ISSUES INCLUDING SUMMARY PLAN DESCRIPTION \(SPD\) REQUIREMENTS AND OTHER DISCLOSURES CONCERNING BLACKOUT PERIODS, PARTICIPANT-DIRECTED DEFINED CONTRIBUTION INVESTMENTS, AND EMPLOYER SECURITY INVESTMENT ALTERNATIVES AND PROSPECTUS REQUIREMENTS](#)

and

#### > [LIMITING LIABILITY UNDER THE ERISA SECTION 404\(C\) AND QUALIFIED DEFAULT INVESTMENT ALTERNATIVE SAFE HARBORS](#)



**RESEARCH PATH:** [Employee Benefits & Executive Compensation > Retirement Plans > ERISA and Fiduciary Compliance > Practice Notes](#)

Training should be provided to investment committee members so they understand ERISA Section 404(a) and 404(c) protections and requirements, including their obligations when selecting "designated investment alternatives" under a Section 404(c) plan, and the plan's QDIA, where applicable. Committee members are not expected to be expert on all matters related to the selection and monitoring of plan investments, but are required to exercise prudence, both in the selection of plan investments and its service providers (which may include retaining experts, like an investment adviser). ERISA § 404(a) ([29 U.S.C. § 1104\(a\)](#)); [29 C.F.R. § 2550.404a-5\(f\)](#). In addition to reviewing plan investment options and service providers, a committee should also be reviewing service provider disclosures to the plan regarding:





- Service provider compensation –and–
- Conflicts of interest (fee disclosures)

See ERISA § 408(b)(2) ([29 U.S.C. § 1108\(b\)\(2\)](#)); [29 C.F.R. § 2550.408b-2](#); [77 Fed. Reg. 5632 \(Feb. 3, 2012\)](#); [79 Fed. Reg. 13949 \(Mar. 12, 2014\)](#). For an additional discussion regarding ERISA fiduciary obligations regarding service provider fee disclosures, see DOL Field Assistance Bulletin (FAB) 2012-2, which provides guidance on the participant-level fee disclosure regulations under Section 404(a)(5) of ERISA (the 404(a)(5) regulation) and the service provider fee disclosure regulations under Section 408(b)(2) of ERISA ([29 U.S.C. § 1108\(b\)\(2\)](#)) (the 408(b)(2) regulation). [FAB 2012-02 \(May 7, 2012\)](#).

#### *Selection of Plan Investment Options*

A committee should be able to demonstrate that it followed a prudent process in selecting, monitoring, and choosing to retain any plan investment option. Process is paramount and a committee should establish, follow, and document its process for investment selection and its ongoing review. In evaluating whether a fiduciary has acted prudently, courts often focus on the process by which the committee gathers information and makes decisions rather than focusing solely on the results of those decisions. (See, e.g., [Krueger v. Ameriprise Fin., Inc.](#), [2012 U.S. Dist. LEXIS 166191 \(D. Minn. 2012\)](#)).

In this regard, when selecting a new or replacing an existing plan investment option, a plan investment committee should:

- Identify the plan investment asset class that it is seeking to fill or review (e.g., an equity mutual fund offering mid-cap exposure).
- Actively seek investment alternatives for consideration that are within that asset class.
  - The committee may wish to hire an investment or pension consultant to assist with this.
- Analyze historical performance of several investment alternatives within the asset class, comparing stated goals, portfolio managers and staff, and fees/costs, against a benchmark investment.
- Following discussion, select the investment option(s) that the committee determines meets (or continues to meet) the plan's needs and execute (or direct the execution of) any agreements required to complete the selection.
- Prepare minutes of the discussion to be reviewed and adopted by the committee at the next meeting.

For an additional discussion regarding committee selection and monitoring of a plan's QDIA investment option(s), see [Dep't of Labor: Target Date Retirement Funds: Tips for ERISA Plan Fiduciaries](#).



### *Asset Classes*

To offer a selection of diverse risk/rewards, a plan wishing to use the ERISA §404(c) safe harbor typically offers funds that fall into these three broad categories:

- Equities
- Fixed income investments (which includes bonds)
- Cash equivalents (which may include very low-risk bonds)

Many large plans also offer an investment brokerage window that enables participants and beneficiaries to select investments beyond those designated by the plan.

### **Benchmarking**

Benchmarking is a key component to monitoring existing plan investments and evaluating new ones. Although ERISA § 404(c) deems a minimum of three investments to constitute a “broad range of investment alternatives,” in practice, defined contribution plans rarely offer so few investment options. A plan may offer five or more QDIA funds alone (when relying upon the “targeted retirement date” safe harbor under [29 C.F.R. § 2550.404c-5\(e\)\(4\)\(i\)](#)), in addition to offering other funds with satisfactorily diverse risk and return profiles. You will typically be looking at a plan with from seven to 15 funds and the committee will need to identify a benchmark for each. However, there is no rule limiting alternatives to any particular number.

Ideally, in determining a proper benchmark the committee should seek to identify an index with attributes similar to the asset in question. Most mutual fund materials identify the benchmarking index used by that fund as is required for participant disclosures under [29 C.F.R. § 2550.404\(a\)-5](#). An investment consultant can also help the committee with this task. Typical benchmarks are Morningstar® or S&P indices established for the same asset class as the portfolio sector.

### **Monitoring Investments**

From a big picture perspective, once the committee is familiar with the different asset classes (and a few other finance fundamentals), you should be in a good position to guide the committee to appropriately consider benchmarking reports prepared by third-party experts. By reviewing these reports the committee can evaluate the performance of each of the plan’s designated investments relative to its associated benchmark. The committee should also seek reports reflecting the percentage of plan assets in each designated investment option and changes over the relative comparative periods. Such reports may illuminate the impact on the plan population should the committee choose to eliminate the investment from the fund lineup.

In addition to reviewing performance against benchmarks, fiduciaries should look at the performance data in the context of applicable macro-environmental factors. [Perez v. Bruister, 54 F. Supp. 3d 629, 660 \(S.D. Miss. 2014\)](#). Any of the following macro factors may have an impact on performance: inflation,

unemployment, interest rates, social conditions, technological changes, legal requirements, and political climate. These factors are part of the reason why past performance is not always an indicator of future performance. These factors may be especially pertinent if the committee is evaluating an international fund's performance.

#### *Use of Comparative Periods*

Committees should consider and evaluate each investment's performance and fees for a sequence of comparative periods (e.g., the most recent quarter, year-to-date, 1-year, 5-year, 10-year periods, or from the shorter fund formation date through the present), also analyzing the rates of return relative to the applicable benchmark indices. In this respect, graphs and charts are useful for committee presentation. In analyzing the data, the committee with its consultant or advisor should look for any trends or sudden changes. If an asset trails the performance of an index, it does not necessarily mean that the committee should immediately remove that asset as an investment option. A committee will often use a watch list (discussed below in "Use of a Watch List") as a monitoring tool for an underperforming investment option. Guidelines should be established as to when to place an investment option on a watch list (e.g., the investment has underperformed its benchmark for three or more consecutive periods). If a watch list option continues to underperform in a material way, the committee may need to consider removing the investment from the plan's investment lineup entirely or eliminate new contributions and exchanges into the fund, or take other appropriate actions. Document the committee's decision for deciding on a particular course of action.

#### *Fee Considerations*

Plan fiduciaries are required to identify, understand, and evaluate fees and expenses relative to plan investment options and service providers. Monitoring plan fees and expenses in light of the services rendered for the plan is a continuing fiduciary responsibility. Proper review of plan investment options often begins with a review of the fee disclosures provided to the plan by service providers as required by ERISA § 408(b)(2) ([29 U.S.C. § 1108\(b\)\(2\)](#)). At least annually then the committee should evaluate fee disclosures for each plan investment option, comparing the fee against a benchmark for investments in the common asset class. This objective benchmarking process should determine:

- How plan costs (fees and expenses) of an investment compare with those of a peer group of investments
- Whether, when evaluating service providers, plan costs are reasonable based on the level of service

## Index Funds

The committee should closely monitor fees for different investment alternatives. It's not uncommon that within the same asset class, for any (higher-cost) actively managed fund, a (lower-cost) index fund is also available. A number of plans offer [index fund](#) options to allow participants to index invest in stocks, bonds, and international equities at lower fees than actively managed funds.

## Fund Classes

Many fund families offer multiple share classes for their funds. While the underlying holdings of a fund may be identical, the fund's expense ratio may be lower for a different class. For example, the committee should consider whether institutional classes of mutual funds (rather than retail mutual funds) are available to the plan from their platform provider. Failure to explore a lower institutional fee structure can attract participant challenges. (See, e.g., [Tibble v. Edison Int'l, 729 F.3d 1110 \(9th Cir. 2013\)](#)).

In particular, if the committee decides not to proceed with the lowest cost option, it should discuss and document its rationale in the meeting minutes. (See, e.g., [Tussey v. ABB, Inc., 746 F.3d 327 \(8th Cir. Mo. 2014\)](#); [Moreno v. Deutsche Bank Ams. Holding Corp., 2016 U.S. Dist. LEXIS 142601 \(S.D.N.Y. Oct. 13, 2016\)](#)).

#### *Use of a Watch List*

A committee may find a watch list of underperforming investment options to be a useful tool when monitoring these investments. An investment alternative is placed on a watch list when the committee determines that a closer review of a particular investment (or service provider) is warranted. Reasons for the additional scrutiny may include:

- The investment is underperforming, usually relative to its designated benchmark, over a designated period (e.g., several quarters).
- The fund manager has changed.
- Negative news regarding the investment or its management appears in fund materials or the media.

Deciding how long an investment option may remain on the watch list before being eliminated may be more art than science. It is generally inadvisable to identify a deadline in the committee charter or investment policy after which a watch list investment should be removed. This compels the committee to follow the directive even if there are special considerations that suggest flexibility. These considerations may include the number of participants or the percentage of plan assets that are invested in the challenged investment.



## Related Content

*For a specific discussion on the service provider disclosures, see*

### > [ERISA SECTION 408\(B\)\(2\) SERVICE PROVIDER DISCLOSURES](#)



**RESEARCH PATH:** [Employee Benefits & Executive Compensation > Retirement Plans > ERISA and Fiduciary Compliance > Practice Notes](#)

*For a broader discussion regarding ERISA fee litigation in individual account plans, see*

### > [401\(K\) PLAN FEE REGULATION AND LITIGATION](#)



**RESEARCH PATH:** [Employee Benefits & Executive Compensation > Retirement Plans > ERISA and Fiduciary Compliance > Practice Notes](#)

*For a sample investment policy statement for a defined contribution plan with participant-directed investments, see*

### > [INVESTMENT POLICY STATEMENT \(DEFINED CONTRIBUTION PLANS\)](#)



**RESEARCH PATH:** [Employee Benefits & Executive Compensation > Retirement Plans > ERISA and Fiduciary Compliance > Forms](#)

*For guidance when selecting an investment manager, see*

### > [INVESTMENT MANAGER HIRING CONSIDERATIONS FOR ERISA PENSION PLANS](#)



**RESEARCH PATH:** [Employee Benefits & Executive Compensation > Retirement Plans > ERISA and Fiduciary Compliance > Practice Notes](#)

## The Importance of Documentation and Legal Counsel

From a practical perspective, while not required, it is often advisable that an ERISA attorney attend committee meetings. The individual will be an advisor to the committee, but not an official member.

An ERISA attorney is uniquely positioned to assist the committee in developing thorough documentation demonstrating the committee's general compliance with ERISA's reasonable prudent person standard. As indicated above, a committee's adherence to processes is vital and results are not necessarily controlling. [Krueger v. Ameriprise Fin., Inc., 2012 U.S. Dist. LEXIS 166191, at 24 \(D. Minn. Nov. 20, 2012\)](#). Written records are critical if later proof is required that the committee satisfied its fiduciary obligations.

For example, an ERISA attorney can assist the committee in ensuring that meeting minutes completely and accurately reflect the committee's rationale for selecting certain investment options, its consideration of reports from third-party experts, voting records of committee members, and its discussion of risk (both with respect to a particular investment and how it would fit into an overall portfolio). Similarly, an ERISA attorney can provide committee members with ongoing fiduciary training and education.

In addition, having an ERISA attorney present at committee meetings is beneficial to timely spot and address potential legal issues. While certain matters clearly indicate the need for a legal opinion, other issues are subtler and nuanced and can easily be missed or inappropriately discounted by non-lawyers.

If the committee does not have an in-house ERISA lawyer as an advisor, trusted external legal counsel should be retained and consulted regularly.

### *Attorney-Client Privilege Considerations*

The committee should have a baseline understanding of attorney-client privilege before engaging an attorney, whether as external counsel, as an official committee member (which is not recommended), or as non-member attorney advisor.

Attorney-client privilege protects communications between a client and its attorney from disclosure to others when the purpose of the communication is to obtain or provide confidential legal advice. An exception applies, however, when counsel provides legal advice to a client who is a fiduciary and concerns the exercise of fiduciary duties. [United States v. Jicarilla Apache Nation, 564 U.S. 162 \(2011\) \(Sotomayor, J., dissenting\)](#); [Becher v. Long Island Lighting Co. \(In re Long Island Lighting Co.\), 129 F.3d 268 \(2d Cir. 1997\)](#).

If an attorney is to be a committee member, note that the individual, in offering advice to the committee, wears the hat of a committee member and not that of the plan sponsor's legal counsel. Thus, attorney-client privilege will not apply with respect to advice offered to the committee and could be discoverable.

The privilege also may not apply if the committee is seeking legal advice from counsel who is not a committee member. Where a committee member requests legal advice from another committee member, the advice is treated as provided to the plan. Courts have ruled that the plan participant or beneficiary can be viewed as the "true client" and attorney-client privilege is unavailable with respect to documentation existing for the discussion or advice. (See, e.g., [McFarlane v. First Unum Life Ins. Co., 231 F. Supp. 3d 10 \(S.D.N.Y. 2017\)](#)). Exercise caution!

As a result, including an attorney as a non-member advisor to the committee (as opposed to an official committee member)



advances, but does not guarantee, preservation of attorney-client privilege.

### The Investment Policy Statement

While not legally required, best practice militates that the committee adopt an investment policy statement (IPS) which outlines the committee's investment philosophy and goals. The IPS should offer sufficient flexibility to react to market conditions while addressing the principles of ERISA's prudent selection and monitoring process, addressing diversification, performance metrics analysis, reasonableness of fees and expenses, etc. An IPS should be concise and understandable.

In turn, the committee must adhere to the terms of the IPS. Taking action contrary to the IPS is generally worse than not having an IPS altogether. If no IPS exists, then whether a committee's behavior constitutes a breach of fiduciary authority could be a question involving greater interpretation of the applicable facts. IPS violations may be used to support a plaintiff's allegations of breach of fiduciary duty.

### Using Investment Experts

The reasonable person prudent standard also applies to engaging experts.

In general, ERISA does not expect fiduciaries to be subject matter experts on all things related to investments. However, fiduciaries must prudently select and monitor experts and may not blindly rely on an expert's advice. [\*Perez v. Bruister\*, 54 F. Supp. 3d 629, 660 \(S.D. Miss. 2014\)](#). Therefore, when hiring and utilizing an expert, the committee should:

- Investigate the expert's qualifications.
  - The committee should pay special attention to an expert's reputation and experience.
- Provide the expert with complete and accurate information.
- Make certain that reliance on the expert's advice is reasonably justified.
  - Committee members should satisfy themselves that expert opinions are supported by relevant materials, reasonable methodologies, and appropriate assumptions.

*Id.* at 661-662.

In certain instances, the committee may appoint an external expert as an ERISA fiduciary. An advisor appointed as an investment manager may be a fiduciary if that investment manager agrees to be identified as such in writing and has the power to manage, acquire, or dispose of any plan assets. ERISA § 3(38) ([29 U.S.C. § 1002\(38\)](#)). That delegation generally relieves



the committee of liability for the investment manager's specific investment decisions. However, even in cases when an investment manager agrees to be a fiduciary, it is imperative that 401(k) plan investment committees adhere to ERISA's overarching principles regarding the prudent and reasonable selection and monitoring of investment options.

### Continuing Education and Training for Committee Members

Continuing education and training are imperative for committee members. Continuing education should cover ERISA fundamentals, such as fiduciary obligations and whether or not an expense is a settlor or plan expense. ERISA § 408(b)(2) ([29 U.S.C. § 1108\(b\)\(2\)](#)); [29 C.F.R. § 2550.408b-2\(b\)](#). For a complete discussion of education recommendations, see the full article on Lexis Practice Advisor.

### Controlling Risk through Insurance

It is best practice, and will make a spot on the committee more appealing, if the plan sponsor purchases fiduciary insurance coverage for committee members. This is different than directors and officers liability insurance, which generally covers

wrongful acts, including actual or alleged errors or neglect or breach of duty on the part of directors in fulfilling their corporate duties. For more information about these policies see the complete article in Lexis Practice Advisor. [L](#)

---

[Jeffrey A. Lieberman](#) is counsel to Skadden, Arps, Slate, Meager & Flom LLP. His practice focuses primarily on fiduciary issues under Title I of ERISA. He regularly counsels asset managers, investment advisors, banks, hedge funds, plan sponsors, pooled investment funds, sponsors of collateralized loan obligations and other securitized vehicles and servicers to such vehicles, issuers of various types of securities, underwriters, and trustees. He also advises private equity fund and other managers as to compliance with ERISA's plan asset regulations and application of the venture capital operating company and other exceptions to the coverage of such funds under ERISA.

---



**RESEARCH PATH:** [Employee Benefits & Executive Compensation](#) > [Retirement Plans](#) > [ERISA and Fiduciary Compliance](#) > [Practice Notes](#)





LexisNexis®

CourtLink®



# REIGN MAKER

RULE NEW BUSINESS WITH  
**COURTLINK®**

*Request a demo*

**[WWW.LEXISNEXIS.COM/REIGNMAKER](http://WWW.LEXISNEXIS.COM/REIGNMAKER)**

**OR CALL 888.253.3901**



**COURT  
COVERAGE**



**SINGLE  
SEARCH**



**NEW CASE  
ALERTS**



**COURTLINK®  
BREAKING COMPLAINTS**



**Ari M. Berman and Laurel S. Fensterstock** VINSON & ELKINS LLP

# Attorney-Client Privilege Considerations for Private Equity Firm Counsel

Private equity investments often present complicated questions concerning the attorney-client privilege, ranging from the interactions between a private equity firm and its portfolio companies to communications with the private equity fund's investors. It is important for in-house counsel at private equity firms to understand what communications likely will be protected and under what circumstances the privilege may be considered to have been waived.

**THIS ARTICLE IS INTENDED TO PROVIDE A HIGH-LEVEL** overview of the attorney-client privilege, identify issues that in-house counsel at private equity firms are likely to face, and provide practice tips for enhancing your chances of preserving the privilege.

## Overview of the Attorney-Client Privilege

The attorney-client privilege is the oldest among the common law evidentiary privileges and protects confidential communications between a client and its attorney made for the purpose of obtaining or providing legal advice. (Courts' analyses of the attorney-client privilege vary according to state and there can be important, and outcome determinative, differences among states. This article is intended to provide a general overview of key principles associated with the privilege as well as those principles' application within the private equity context.) The purpose of the privilege is to encourage full and frank dialogue between lawyers and clients, and communications protected by the privilege need not be disclosed in litigation. [Upjohn Co. v. United States](#), 449 U.S. 383, 389, 101 S. Ct. 677, 682, 66 L. Ed. 2d 584 (1981); [Spectrum Sys. Int'l Corp. v. Chem. Bank](#), 78 N.Y.2d 371, 377, 581 N.E.2d 1055, 1059 (1991).



To be privileged, a communication essentially must be primarily or predominantly of a legal—rather than a business—character. The critical inquiry is whether the communication was made in order to render legal advice or services to the client. [Spectrum Sys. Int'l](#), 581 N.E.2d at 1061. A communication will be protected where it concerns legal

**WHERE TWO OR MORE CLIENTS SEPARATELY ENGAGE THEIR OWN COUNSEL  
TO ADVISE THEM ON MATTERS OF COMMON LEGAL INTEREST,  
THE COMMON INTEREST EXCEPTION ALLOWS THEM TO SHIELD FROM DISCLOSURE  
CERTAIN ATTORNEY-CLIENT COMMUNICATIONS THAT ARE REVEALED TO ONE  
ANOTHER FOR THE PURPOSE OF FURTHERING A COMMON LEGAL INTEREST.**

rights and obligations and demonstrates other professional skills, such as a lawyer's judgment and recommended legal strategies. *Rossi v. Blue Cross & Blue Shield of Greater N. Y.*, 73 N.Y.2d 588, 594, 540 N.E.2d 703, 706 (1989).

As a general matter, courts tend to scrutinize more closely communications with in-house counsel than outside counsel—guided by the principle that the privilege is not meant to be used as a shield to protect otherwise discoverable information. This is due primarily to the fact that in-house lawyers often have mixed legal and business responsibilities and can wear multiple hats, including serving as company officers. During their day-to-day interactions, in-house lawyers often walk the line between legal and non-legal involvement in company affairs—and that line can easily, and inadvertently, get blurred. Courts have warned that the mere participation of an in-house lawyer does not automatically protect communications from disclosure. *Rossi*, 540 N.E.2d at 705.

### **Privilege Challenges Facing In-House Counsel**

In the private equity context, issues relating to the attorney-client privilege may arise in various scenarios, including when (1) a private equity firm's employee plays multiple roles, (2) one lawyer or law firm represents two clients, (3) clients share a common legal interest, and (4) there is a sale of a portfolio company.

### **Multiple Roles of Private Equity Professionals**

Private equity firms commonly designate employees to serve as members of the boards of directors of portfolio companies. These designees wear two hats—one as employees of the private equity firm and the other as members of portfolio companies' board of directors. If a portfolio company shares privileged information (e.g., advice provided by the portfolio company's outside or in-house counsel) with an individual in his capacity as a director, the attorney-client privilege should be preserved. However, if that individual subsequently shares the privileged communication with his private equity colleagues in his capacity as an employee of the private equity firm, there is a risk that the attorney-client privilege could be considered to have been waived. (Generally, when a client

shares privileged information with a third party, the attorney-client privilege will be waived.) In addition to being trained with respect to fiduciary duties owed to portfolio companies, private equity director designees should be sensitized to the issue of preserving portfolio companies' privilege.

### **Joint-Client Theory**

The joint-client or co-client theory applies when one attorney represents the interests of two or more entities on the same matter, including where a parent corporation and one of its subsidiaries consult the same counsel with respect to a common legal cause. See, e.g., *Bass Pub. Ltd. Co. v. Promus Cos. Inc.*, 868 F. Supp. 615 (S.D.N.Y. 1994). Each respective joint client's communications with common counsel are protected by the attorney-client privilege, and if such communications are shared with another joint client, the privilege should be preserved. (Waiving the joint-client privilege typically requires the consent of all joint clients. A joint client may unilaterally waive the privilege as to its own attorney-client communications, so long as those communications concern only the waiving client. Such client may not unilaterally waive the privilege as to any of the other joint clients' communications or as to any of its communications that relate to other joint clients. *In re Teleglobe Commc'ns Corp.*, 493 F.3d 345, 363 (3d Cir. 2007)). Whether two clients qualify as joint clients depends primarily on the understanding of the parties and the lawyer in light of the circumstances, including the details of the representations and the clients' interaction with the attorney and each other. *In re Teleglobe Commc'ns*, 493 F.3d at 363 (citing *Sky Valley Ltd. P'ship v. ATX Sky Valley Ltd.*, 150 F.R.D. 648, 652–53 (N.D. Cal. 1993)).

There is not well-developed case law applying joint-client principles to the private equity context (i.e., to communications between a private equity firm and a portfolio company that shares the same lawyer). Accordingly, it is important to proceed with caution when relying on the joint-client theory and make clear in engagement letters with outside counsel that such representation will be on a joint-client basis.



**... IN-HOUSE COUNSEL SHOULD KEEP THEIR LEGAL FILES AND BUSINESS FILES SEPARATE FROM ONE ANOTHER, AND UTILIZE CONFIDENTIALITY DESIGNATIONS TO MAKE CLEAR WHAT IS CONSIDERED LEGAL ADVICE VERSUS PURE BUSINESS ADVICE.**

### Common Interest Exception

Common interest is an exception to the general rule that the presence of a third party will destroy a claim of privilege. Where two or more clients separately engage their own counsel to advise them on matters of common legal interest, the common interest exception allows them to shield from disclosure certain attorney-client communications that are revealed to one another for the purpose of furthering a common legal interest. [Ambac Assur. Corp. v. Countrywide Home Loans, Inc.](#), 27 N.Y.3d 616 (N.Y. 2016). This exception historically has been applied in the merger context. For instance, where parties were represented by separate counsel and a merger agreement directed them to share privileged information relating to pre-closing legal issues, courts generally had found that such

disclosure did not waive the privilege—reasoning that the parties shared a common legal interest and the communication was designed to further that interest. However, in a recent decision, the New York Court of Appeals made clear that such a fact pattern would waive the attorney-client privilege, unless the sharing of information was made in connection with pending or reasonably anticipated litigation. *Id.* Making matters even more complicated is that jurisdictions differ on whether litigation must be pending or reasonably anticipated—and it can be difficult to analyze which state’s law should govern a particular transaction. Accordingly, in-house counsel should use caution and anticipate that the common interest exception may not apply to these types of communications (especially considering the recent uptick in merger-related lawsuits).

The common interest exception also may apply in the context of a communication between the private equity firm and its investors concerning a threatened or ongoing litigation or investigation. Much like communications including portfolio companies, these interactions require careful analysis due to the risk of waiver (i.e., the potential that the private equity firm loses the privilege by sharing privileged information with one or more limited partners).

### Sale of a Portfolio Company

When control of a company passes to new management, whether through a sale, merger, takeover, or normal succession, the authority to assert and waive the company’s attorney-client privilege also passes to new management. [Bass Pub. Ltd.](#), 868 F. Supp. at 619 (citing [Commodity Futures Trading Comm’n v. Weintraub](#), 471 U.S. 343, 349, 105 S. Ct. 1986, 1991, 85 L.Ed.2d 372 (1985)). If a company that acquires a portfolio company from a private equity firm later sues the private equity firm, the acquirer may be able to access and use in the litigation legal advice that the private equity firm and its former portfolio company received jointly. Thus, it is important to limit the joint representation of a private equity firm and its portfolio companies to instances in which it is necessary. And, consideration should be given to whether it makes sense to retain separate counsel for purposes of any contemplated sales/purchases in an effort to limit the amount of privileged communication that can be passed to new management.

### Practice Tips

**Think ahead.** While privileged communications are not likely to be challenged until litigation, it is important to follow best practices to ensure a private equity firm and its portfolio companies are in a strong position to defend the privileged status of its communications. Think about the extent to which the privilege may or may not apply to a particular communication with a portfolio company or investor in the fund.

### Related Content

For assistance in drafting a side letter to be used when forming a private equity fund, see

> [SIDE LETTER FOR A PRIVATE EQUITY FUND](#)



**RESEARCH PATH:** [Corporate and M&A > Private Equity > Fund Formation and Operation > Forms](#)

For more information on fee and expense disclosure and documentation for private equity funds, see

> [PRIVATE EQUITY FEE AND EXPENSE DISCLOSURE](#)



**RESEARCH PATH:** [Corporate and M&A > Private Equity > Fund Reviews and Limited Partner Negotiations > Practice Notes](#)

For an overview of the various remedies that investors typically negotiate for when investing in a private equity fund, see

> [INVESTOR REMEDIES](#)



**RESEARCH PATH:** [Corporate and M&A > Private Equity > Fund Formation and Operation > Practice Notes](#)



**Separate business from legal.** To the extent possible, in-house counsel should keep their legal files and business files separate from one another and utilize confidentiality designations to make clear what is considered legal advice versus pure business advice. Be wary, however, of overuse of such confidentiality designations—a document that is labeled “privileged and confidential” may not be considered as such if there is no actual legal advice being sought or communicated.

**Make your position clear.** Make clear when in-house lawyers are acting in a legal versus business capacity. In meetings or conference calls, in-house counsel should announce their role as legal advisor when appropriate or document in minutes of meetings that the discussions were had for the purpose of providing legal advice. In-house counsel’s presence on a call, a meeting, or e-mail chain, by itself, is not likely to establish that the communication is privileged.

**Make any joint-client relationship clear in an engagement letter.** When the joint-client theory is a portfolio company’s basis for asserting that sharing privileged information with a private equity firm does not waive privilege, such expectation should be laid out in an engagement letter with the law firm that clearly sets out the scope of the joint representation. Further, agreements between the private equity firm and its

portfolio company should provide that privileged information will be shared among the parties as co-clients and must be kept confidential and not shared with any third parties.

**Keep those with multiple roles aware of the risk.** Educate employees who serve as designees on boards of portfolio companies of the risks associated with sharing privileged information belonging to the portfolio company with others at the private equity firm.

**Take steps to maintain privilege.** When possible, disseminate privileged information only to those who need to know, (i.e., those who need to know the content of the communication to perform their job effectively or to make informed decisions concerning the subject matter of the legal communication). Instruct those with access to privileged information to avoid disclosing such information to others.

**Tailor inspection rights.** Consider tailoring inspection rights to permit a portfolio company to withhold privileged information from the private equity firm where no joint-client or other shared privilege applies.

**Maintain confidentiality.** Take steps to ensure that portfolio companies’ privileged information shared with the private equity firm as co-client is kept confidential.

**Use separate counsel when concerned about potential post-sale litigation by purchasers.** If concerned about the possibility of post-sale litigation, be wary of relying upon the joint-client theory to protect privileged communications from disclosure to the acquirer. Consult separate legal counsel for issues the firm does not want a potential acquirer to learn about or communicate with the portfolio company's outside counsel separately, as a separate client, to ensure it receives its own legal advice. For added security, consider including in sale/merger agreements a provision that expressly addresses the transfer of ownership of privileged communications.

By taking care to properly identify privileged communications and implement thoughtful policies and procedures, private equity firms should be able to successfully balance minimizing the risk of waiver with the commercial goal of effectively managing its investments. **L**

---

**Ari M. Berman** is a partner at Vinson & Elkins, LLP. His main area of practice is commercial litigation, with an emphasis on lawsuits involving the federal securities laws. He has significant experience representing companies and individuals—including public companies, financial institutions, private investment funds, and officers and directors—in contexts such as investigations and enforcement proceedings by the SEC, FINRA, and other law enforcement and regulatory agencies. **Laurel S. Fensterstock** is a commercial litigator whose practice focuses on complex business disputes in both state and federal courts, including breach of contract, intellectual property, securities litigation, and bankruptcy litigation. She also has experience representing clients in foreign arbitrations and internal investigations.

---



**RESEARCH PATH:** [Corporate and M&A > Private Equity](#)  
[> Fund Reviews and Limited Partner Negotiations >](#)  
[Practice Notes](#)





**Devika Kewalramani** MOSES & SINGER LLP

# In-House Counsel Ethics: Fee Sharing Implications

Lawyers are prohibited from sharing legal fees with non-lawyers unless an exception applies. The issue of fee sharing infrequently arises for in-house counsel as they are typically salaried employees who usually do not receive fees for advising their corporate employers.



**ON THE RARE OCCASION THAT IN-HOUSE ATTORNEYS** represent their employer-client in litigation and arbitration matters, ethical issues involving fee sharing and the unauthorized practice of law may be implicated. [N.Y. State Ethics Opinion 1121](#) (Opinion 1121 issued by the New York State Bar Association, Committee on Professional Ethics (the Committee) in May 2017<sup>1</sup> dealt with two issues:

(1) whether in-house counsel for a company may remit the entire attorney's fee portion of an arbitration award to the claimant company without violating the fee-sharing rule and (2) whether remittal of attorney's fees to its corporate employer would constitute aiding the non-lawyer company in the unauthorized practice of law.

<sup>1</sup> [New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 1121 \(2017\)](#).

## ON THE RARE OCCASION THAT IN-HOUSE ATTORNEYS REPRESENT THEIR EMPLOYER-CLIENT IN LITIGATION AND ARBITRATION MATTERS, ETHICAL ISSUES INVOLVING FEE SHARING AND THE UNAUTHORIZED PRACTICE OF LAW MAY BE IMPLICATED.

In [Opinion 1121](#), the inquiring in-house counsel was employed by a corporation that provided medical equipment to individuals through prescribing physicians. In-house counsel handled general corporate matters and arbitrations involving denial of insurance claims and occasionally litigated them. If the claimant corporation made a monetary recovery resulting from the arbitration, the amount would be bifurcated with a portion of the award being paid for (1) the incorrect denial by the insurance provider for the medical equipment and (2) attorney's fees awarded to the attorney-of-record. Industry practice required the paying insurance companies to distribute the attorney's fees award to the attorney-of-record and not directly to the corporation. After receipt by the attorney-of-record, the only means by which the employer-corporation could recover the attorney's fees was by way of sharing fees.

The Committee previously analyzed the fee-sharing prohibition in Rule 5.4(a) of the New York Rules of Professional Conduct ([NY Rule 5.4\(a\)](#))<sup>2</sup> in its earlier ethics opinions involving remitting attorney's fees to a non-lawyer client or employer. For example, [N.Y. State Ethics Opinion 906](#) (Opinion 906)<sup>3</sup> barred an in-house lawyer from sharing legal fees awarded in litigation with a not-for-profit organization, based on [NY Rule 5.4\(a\)](#). There, although the lawyer was employed by the not-for-profit organization that represented third parties, the lawyer was not representing the not-for-profit organization itself. The Committee noted that [New York Rule 5.4\(a\)](#) is different from [ABA Model Rule 5.4\(a\)\(4\)](#), which expressly permits a lawyer to share court-awarded attorney's fees with a non-profit public interest organization where the lawyer prevailed in a litigated matter on behalf of the organization. The Committee distinguished [Opinion 906](#), where the in-house lawyer proposed to share fees not with the client who won fees for itself, but rather with the not-for-profit entity sponsoring the litigation on behalf of the prevailing third party. In contrast, [N.Y. State Ethics Opinion 1096](#)<sup>4</sup> found that the fee-sharing rules were not violated because the statutory fees were awarded to the non-lawyer prevailing party/client rather than directly to the lawyer.

Based on the above, [Opinion 1121](#) concluded that in-house counsel here was employed by the prevailing party and litigated the claim on behalf of its for-profit employer and not on behalf of third parties, thereby permitting counsel to share the attorney's fee portion of the award with its non-lawyer employer, without violating [NY Rule 5.4\(a\)](#). Additionally, New York no-fault insurance law and the applicable American Arbitration Association rule provided that the claimant (i.e., the corporation by way of subrogation) was entitled to payment of all components of the award, including attorney's fees, even if the actual check for attorney's fees was made payable to the attorney-of-record.

Finally, the Committee addressed whether remitting the attorney's fees to the non-lawyer employer would violate

### Related Content

For more on trends related to sanctions, see

#### > [IN-HOUSE COUNSEL SANCTIONS: RECENT TRENDS](#)



**RESEARCH PATH:** [Corporate Counsel > Ethics for In-House Counsel > Conflicts of Interest > Articles](#)

For a discussion of how to spot ethical challenges, see

#### > [IDENTIFYING CONFLICTS OF INTEREST](#)



**RESEARCH PATH:** [Corporate Counsel > Ethics for In-House Counsel > Conflicts of Interest > Practice Notes](#)

For information on disqualification of in-house counsel resulting from a conflict of interest, see

#### > [IN-HOUSE COUNSEL DISQUALIFICATION: RARE BUT REAL](#)



**RESEARCH PATH:** [Corporate Counsel > Ethics for In-House Counsel > Conflicts of Interest > Articles](#)

2. New York Rules of Prof'l Conduct R. 5.4 (2017). 3. New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 906 (2012). 4. New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 1096 (2016).



Rule 5.5(d) of the New York Rules of Professional Conduct ([NY Rule 5.5\(d\)](#)),<sup>5</sup> which prohibits a lawyer from aiding a non-lawyer in the unauthorized practice of law. It noted that whether a particular activity constitutes the unauthorized practice of law is a legal question outside the Committee's jurisdiction. However, the Committee pointed out that [Section 495 of the New York Judiciary Law](#) might apply: first, [Section 495\(2\)](#) permits a moneyed corporation authorized to do business in New York to receive an assignment of claim under a subrogation agreement, and second, [Section 495\(5\)](#) allows a corporation to employ attorneys in its own immediate affairs or in any litigation to which it is a party.<sup>6</sup>

[Opinion 1121](#) provides guidance on how in-house counsel may serve their corporate employer without bending or breaking the ethics rules. This may be a growing trend. With the increasingly expanding role of in-house counsel today, where they are on

the front lines of litigation and arbitration involving their corporate clients, ethics issues will inevitably be on the upswing. These issues tend to be complex and require careful scrutiny of many factors and circumstances surrounding in-house counsel's activities, roles, and responsibilities. **L**

---

[Devika Kewalramani](#) is a partner at Moses & Singer LLP and co-chair of its Legal Ethics & Law Firm Practice. Ms. Kewalramani focuses her practice on legal ethics, professional discipline, risk management, and compliance. She serves as the chair of the Committee on Professional Discipline of the New York City Bar Association.

---



**RESEARCH PATH:** [Corporate Counsel > Ethics for In-House Counsel > Practice Notes](#)

---

5. [New York Rules of Prof'l Conduct R. 5.5 \(2017\)](#). 6. [N.Y. Jud. Law § 495 \(LexisNexis 2017\)](#).





**Lori Zyskowski** GIBSON, DUNN & CRUTCHER LLP

# Market Trends: Responding to Negative Voting Recommendations by Filing Additional Proxy Soliciting Materials

The voting recommendations of proxy advisory firms—including, most notably, Institutional Shareholder Services (ISS) and Glass Lewis & Co. (Glass Lewis)—continue to influence the voting outcomes of company and shareholder proposals. Even when the company's largest shareholders follow their own voting policies, the voting recommendations of proxy advisory firms can be influential on the voting outcome.

## **WHEN FACED WITH A NEGATIVE VOTING RECOMMENDATION,**

to the extent the recommendation is not based on an error that can easily be corrected, most companies elect to file additional proxy soliciting materials along with engaging directly with shareholders to explain their side of the story or to potentially address the underlying issue that led to a negative vote recommendation. This article principally explores the practice (and effectiveness) of responding to negative vote recommendations from proxy advisory firms by filing additional definitive proxy soliciting materials with the Securities and Exchange Commission (SEC). As discussed in greater detail below, a decision whether to file additional proxy soliciting materials is specific to each company's individual circumstances. In addition, in an era of sharpened focus on shareholder engagement, some companies file additional proxy soliciting materials in connection with their annual shareholder meetings as part of their ongoing shareholder engagement strategy. Given these trends, companies will continue to file additional proxy soliciting materials, both regularly as part of their annual proxy solicitation process, and on special occasions, such as when they seek to respond to a negative voting recommendation from one or more proxy advisory firms.



## **Legal Requirements**

When faced with a negative voting recommendation on a company proposal or one or more director nominees, companies typically want to convince their shareholders that voting in line with the board's recommendations is

appropriate. However, shareholder outreach while a proxy solicitation is being conducted must be carefully managed to avoid violating the SEC's proxy solicitation rules. Specifically, under Section 14(a) ([15 U.S.C. § 78n](#)) of the Securities Exchange Act of 1934, as amended, and Rule 14a-6 ([17 C.F.R. § 240.14a-6](#)), public companies are required to file any "soliciting" materials that could be deemed to be "written" communications related to the matters to be voted on at the annual meeting. As such, the primary benefit of filing additional soliciting materials is to facilitate shareholder outreach by allowing companies to communicate directly with shareholders about their proposals while complying with proxy solicitation rules.

### What Must Be Filed?

The SEC's rules define solicitation broadly; the definition includes "[t]he furnishing of a form of proxy or other communication to security holders under circumstances reasonably calculated to result in the procurement . . . of a proxy." Therefore, companies should generally file any written communications or materials given to shareholders (whether by mail, e-mail, or in one-on-one meetings) and other groups (if designed to influence the vote) related to the proxy statement or matters to be voted on at the annual meeting. Examples include:

- Press releases (e.g., related to shareholder proposals, Glass Lewis, or ISS)
- Shareholder letters and any materials (e.g., slide presentations) used in one-on-one meetings with shareholders
- E-mails and other written materials furnished to employees that comment on the proxy solicitation or that encourage employees to vote as recommended by the board
- Talking points or scripts used internally or provided to proxy solicitors to contact shareholders and urge them to vote
- Transcripts of audio and video presentations, if made available for playback after the initial presentation (and any such playback should not be made available until a transcript has been filed)

Filing additional soliciting materials is relatively simple as it involves only an SEC Schedule 14A cover page plus whatever soliciting materials will be used or distributed. They appear in the SEC's EDGAR electronic filing system as DEFA14A filings.

Importantly, in addition to the SEC's solicitation rules, companies should also keep in mind Regulation FD ([17 C.F.R. § 243.100-103](#)) (which prohibits selective disclosure of material, nonpublic information to a shareholder under circumstances in which it is reasonably foreseeable that the shareholder will purchase or sell the company's securities

on the basis of that information) and Rule 14a-9 ([17 C.F.R. § 240.14a-9](#)) (which prohibits making materially false and misleading statements in connection with proxy solicitations). As such, all levels of the company should be urged to involve the legal department in all possible meeting-related communications to assess possible filing requirements.

### What is the Timing of Filing Additional Soliciting Materials?

Filings are due at the same time communications are sent or provided to shareholders. The release and filing of written materials (e.g., press releases, web postings, or shareholder letters) therefore needs to be coordinated.

### What Does Not Need to Be Filed?

Even though soliciting material is broadly interpreted, the following are typically not required to be filed under SEC rules:

- Purely oral conversations as long as they do not consist of reading from a script during calls with investors (e.g., internal talking points that are not read verbatim typically do not constitute scripts and do not need to be filed)
- Internal briefing materials used to prepare for meetings with shareholders and proxy advisory firms
- Internal Q&As used in response to unsolicited inquiries that address specific questions
- Transcripts of purely oral communications that are not made available for playback

In addition, no filing is typically required if the company is providing information that is within the four corners of what has been previously publicly filed by the company. As such, the company may consider filing a broad set of talking points or other additional soliciting materials relatively early on in the process. Such materials may help minimize the number of subsequent supplemental filings.

## Other Benefits and Considerations

### What Are Some Other Benefits of Filing Additional Proxy Soliciting Materials in Response to Negative Voting Recommendations?

In addition to complying with the legal requirements, additional proxy soliciting materials can be useful for a variety of other reasons, including:

- **Foundation for shareholder engagement.** Additional proxy soliciting materials can provide a foundation for shareholder engagement by providing the appropriate context and focusing the discussion on the core issues. In addition, such additional proxy soliciting materials reflect a larger overall trend—companies choosing to communicate directly with shareholders on a more consistent basis.



- **Basis for investor support.** Many institutional investors have their own proxy voting guidelines that they follow. Consequently, they may be persuaded by the arguments reflected in a company's additional proxy soliciting materials. For other investors, proxy voting personnel or portfolio managers can rely on the additional proxy soliciting materials that are a part of the public record if they choose to override a proxy advisory firm's recommendation or make their case before a proxy committee.
- **Additional information for proxy advisory firms.** As discussed in greater detail below, proxy advisory firms will only take into account publicly available information (including in circumstances where a company would like a proxy advisory firm to reverse its negative voting recommendation). Additional soliciting materials (which is how the annual meeting-related information is typically relayed once the proxy statement is filed) are effectively a prerequisite for getting proxy advisory firms to consider additional information for purposes of changing their voting recommendations.

#### **Should a Company Always File Additional Proxy Soliciting Materials in Response to a Negative Voting Recommendation?**

The various proxy advisory firms have different approaches for evaluating company and shareholder proposals. As a result, it is not uncommon for companies to get a favorable recommendation from one advisory firm, while receiving a negative recommendation from another. In addressing such split recommendations, companies need to understand the makeup of their shareholder base and recognize that ISS recommendations may carry more weight with investors than recommendations from Glass Lewis or other proxy advisory firms because ISS is more widely followed. If a company receives a favorable recommendation from ISS and a negative recommendation from Glass Lewis or another proxy advisory firm, the company may not find it advisable to openly address the negative recommendation by filing additional proxy soliciting materials with the SEC, especially because doing so could draw more attention to the negative recommendation than would otherwise be the case. In evaluating whether additional soliciting materials might be warranted, a company should consult with its proxy solicitor to determine how many of its major shareholders follow the voting recommendations



**OUTSIDE OF THE SAY-ON-PAY SPACE, TO THE EXTENT ADDITIONAL SOLICITING MATERIALS ARE MEANT TO ADDRESS A SPECIFIC ISSUE (SUCH AS A BYLAW AMENDMENT OR DISCLOSURE AROUND MATERIAL INTERNAL CONTROL WEAKNESSES), THEY TEND TO BE RELATIVELY LIMITED IN SCOPE TO THE TOPIC IN QUESTION.**

of a particular proxy advisory firm. To the extent that such shareholder base is not significant, the company may determine that it is better to wait to address the issues in the company's next proxy statement.

### **Preparing Effective Additional Proxy Soliciting Materials**

#### **What Do Additional Soliciting Materials Filed in Response to Negative Voting Recommendations Typically Look Like?**

Additional soliciting materials filed in response to a negative voting recommendation can take various forms. The most common formats include:

- A letter, either to shareholders or a proxy advisory firm (e.g., Allstate Corp.'s DEFA14A, filed April 11, 2011; Allergan plc's DEFA14A, filed April 19, 2016)
- A presentation (e.g., Morgan Stanley's DEFA14A, filed April 27, 2016)
- Talking points (e.g., Johnson Controls International plc's DEFA14A, filed February 22, 2011)

While less common, they can also take a form of website pages, e-mail correspondence, and scripts.

#### **What Do Additional Proxy Soliciting Materials Filed in Response to Negative Voting Recommendations Typically Address?**

##### *Say-on-Pay Proposals*

Semler Brossy, an executive compensation consulting firm, has been tracking additional proxy soliciting materials filed in response to negative say-on-pay recommendations from proxy advisory firms since 2011. The number of such additional proxy soliciting materials has declined substantially since 2011, even though the percentage of companies receiving a negative voting recommendation from ISS has remained relatively constant (12% in 2016 and 12.5% in 2011). This is likely because Semler Brossy's data also indicates that company responses via additional proxy soliciting materials to a negative voting recommendation do not have a material impact on voting results. Moreover, while a say-on-pay vote is by no means routine, most companies are now familiar with the voting

methodologies of proxy advisory firms when it comes to say-on-pay proposals and generally understand how to approach their say-on-pay votes in both good and bad years.

According to Semler Brossy, only 35 additional proxy soliciting materials responding to a negative say-on-pay voting recommendation were filed in 2016 (as compared to 59 in 2011 and 113 in 2012). Such materials typically address the following key topics, with pay-for-performance being addressed in more than 70% of such additional soliciting materials in each year since 2011:

- Pay-for-performance relationship (i.e., arguing that the executive compensation is in line with the company's financial performance)
- Peer group comparators
- Proxy advisor methodology (i.e., arguing that such methodology is faulty or does not take into account an important factor in the company's case)
- Factual errors
- Timing of grants (i.e., arguing that the equity awards received during the year in which performance suffered were for performance for the prior year even though SEC rules require disclosure of equity grants in the year in which grants have been made)
- Governance highlights (i.e., highlighting a company's other good governance practices in addition to responding to specific executive compensation-related issues identified by a proxy advisory firm)
- Realizable pay (defined under ISS guidelines as including the cash and benefit values actually paid, and the value of any amounts realized (i.e., exercised or earned due to satisfaction of performance goals) from incentive grants made during a specified measurement period, based on their value as of the end of the measurement period)
- Program changes following proxy advisory firm's recommendation

### *Other Issues*

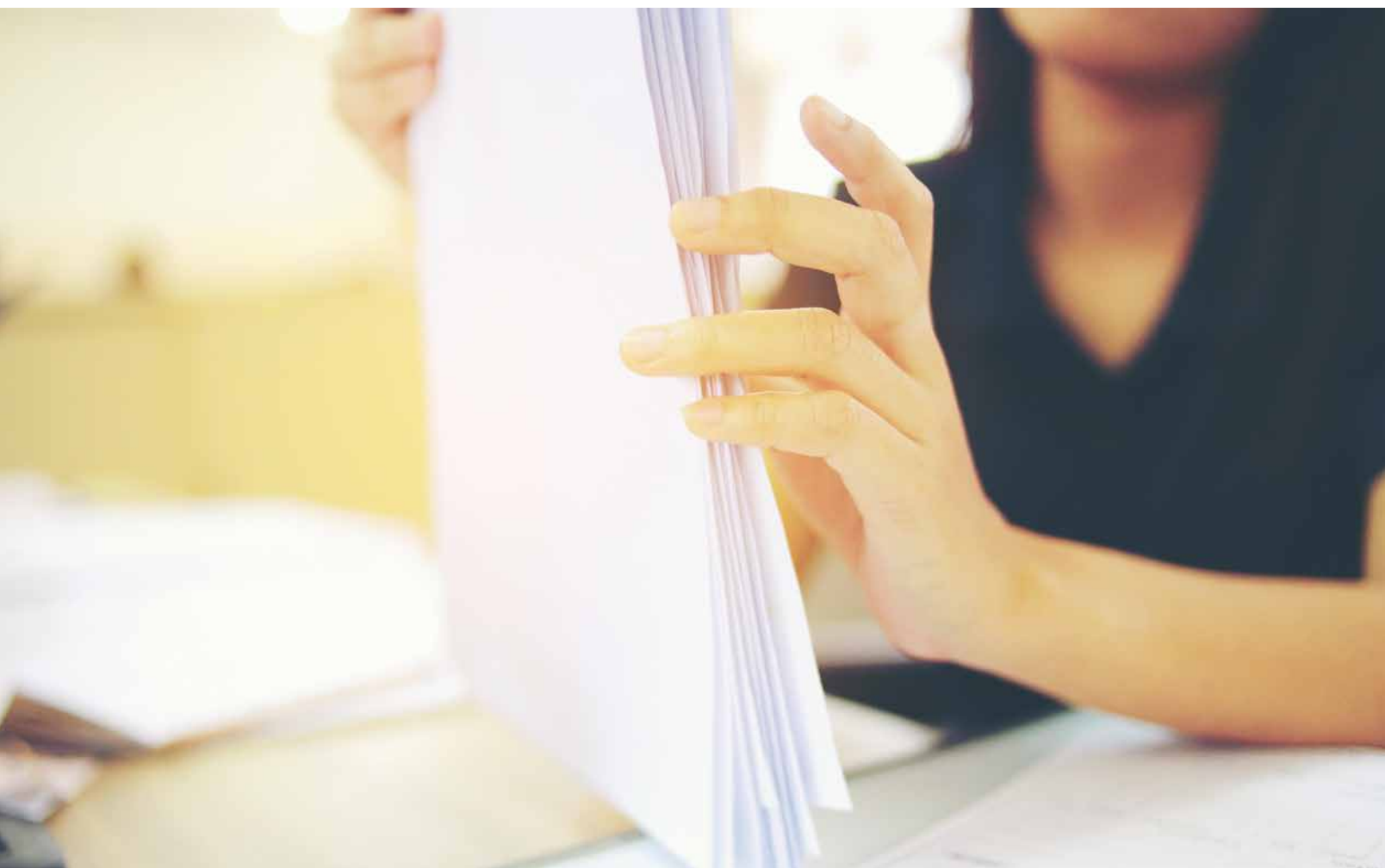
Outside of the say-on-pay space, to the extent additional soliciting materials are meant to address a specific issue (such as a bylaw amendment or disclosure around material internal control weaknesses), they tend to be relatively limited in scope to the topic in question. For instance, additional soliciting materials that are intended to disclose that a non-independent director (under the proxy advisory firm's standards) has resigned from the public company's key committees might be limited to one sentence disclosing precisely that. Such additional soliciting materials are simple and to the point.

If the issue is more complex (such as a proxy advisory firm supporting a shareholder proposal that could impact the company's leadership structure or require the company to incorporate in a different state), a company may choose to include a more detailed explanation of why shareholders should vote in line with the board's recommendations, as opposed to recommendations of a proxy advisory firm. Typically, such additional soliciting materials would also highlight the company's good governance practices in addition to addressing the subject or issue that led to a negative voting recommendation.

### **What Additional Proxy Soliciting Materials Are the Most Effective?**

To the extent additional soliciting materials address more complex topics (such as say-on-pay proposals), it is better to counter the proxy advisory firms' arguments through the careful presentation of countervailing evidence and/or a compelling story rather than by openly criticizing the proxy advisory firms and their proxy voting practices or guidelines. At a high level, the most effective additional proxy soliciting materials that are not meant to address specific/simple issues do the following:

- **Provide extra details, while highlighting the positives.** The parameters of this strategy would depend, in part, on when additional proxy soliciting materials are filed. If they are filed after a negative voting recommendation is received, the company might choose to focus on one or two specific issues. If they are filed before the negative voting recommendation is received, the company might take a different approach and tell its story by emphasizing certain aspects of its compensation program and governance practices. In either case, additional proxy soliciting materials that emphasize the positives seem to be more effective than those that focus solely on refuting the proxy advisory firms' criticisms.



- **Keep the narrative simple.** As noted above, many additional proxy soliciting materials take the form of a letter or presentation. These should not be overly complicated or long. Investors are already getting tired of looking at extensive proxy statements, which is why it is important to keep the narrative simple and focused.
- **Leverage split recommendations or other third-party information.** To the extent that a company receives a split voting recommendation and decides to file additional proxy soliciting materials, it may help the company's argument to discuss the fact that another proxy advisory firm issued a different voting recommendation. References to other third-party resources could be effective as well. For instance, if a company is opposing a political contributions proposal, but has a good score in the CPA-Zicklin Index (which benchmarks the political disclosure and accountability of public corporations), that could be an important fact to highlight.

## How to Reverse Negative Voting Recommendations

### Can a Negative Voting Recommendation Be Reversed?

In order to ensure consistency, the proxy advisory firms' policies are generally inflexible by necessity. That means that it is not easy to get a proxy advisory firm to reverse its voting recommendation once it is public, even with the most well-written additional proxy soliciting materials. However, this does not mean that doing so is impossible. In all cases, companies should focus their efforts on reaching their shareholders. In other words, even if additional soliciting materials are not sufficient to sway a proxy advisory firm, they may be sufficient to sway enough of the institutional investors who have more flexible voting policies and do not uniformly vote with the recommendations of the proxy advisory firms.

ISS

ISS generally issues U.S. company proxy reports 13 to 25 calendar days before the shareholders meeting. In the United States, companies in the S&P 500 can elect to receive a draft of their ISS report for fact-checking purposes before it is distributed to ISS's clients. Therefore, an S&P 500 company should review its draft report and notify ISS of any inaccuracies or other comments by e-mail at [usresearch@issgovernance.com](mailto:usresearch@issgovernance.com). Similarly, other companies should contact ISS as soon as possible after the final report is issued if any errors are found. All companies can access ISS's proxy analyses of their company without charge through an ISS governance analytics platform (for which companies must obtain log-in information in advance). Once the report is final, if ISS agrees there is an error, it will issue a proxy alert to its clients. Companies are more successful in receiving revised recommendations when

they can demonstrate that ISS made an irrefutable factual error (for example, where the ISS recommendation is based on the assumption that the compensation plan has single-trigger acceleration for vesting of outstanding awards, when, in fact, it has double-trigger acceleration).

Notably, it is critical that companies address inaccuracies promptly because ISS generally will not change its voting recommendations within five business days of the company's annual meeting. New information received within the five business days before the meeting will be set forth in an informational alert if ISS determines it is material to the proxy analysis but will not result in a revised voting recommendation.

### Related Content

For additional information on proxy advisory firms, see

#### > [UNDERSTANDING THE ROLE OF PROXY ADVISORY FIRMS](#)

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Proxy Statement and Annual Meeting > Mailing and Delivery of the Proxy Statement > Practice Notes](#)

For further information on proxy solicitation and the contents of an annual report, see

#### > [DRAFTING THE PROXY STATEMENT AND ANNUAL REPORT](#)

 **RESEARCH PATH:** [Corporate Counsel > Shareholder, Board and Company Actions > Proxy Statements and Annual Meetings > Practice Notes](#)


For a set of guidelines and questions to consider for a policy with respect to shareholder engagement and communications, see

#### > [BOARD ENGAGEMENT WITH SHAREHOLDERS POLICY CHECKLIST](#)

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Corporate Governance and Compliance Requirements for Public Companies > Corporate Governance > Checklists](#)

For an overview on say-on-pay votes, see

#### > [COMPLYING WITH DODD-FRANK'S SAY-ON-PAY PROVISIONS](#)

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Executive Compensation > Corporate Governance Issues > Practice Notes](#)



ISS will issue an alert to change a voting recommendation closer than five business days before the meeting only under “highly extraordinary circumstances.”

Outside of an objectively verifiable error (that can and must be proved by referring to publicly available proxy materials), it is difficult to get ISS to reverse its voting recommendation, although it is still possible. Outlined below are typical considerations and steps for a company that is seeking to have ISS reverse its voting recommendation:

■ **In limited circumstances, consider reaching out to ISS.**

If the reasons for a negative voting recommendation are not entirely clear, a company may want to reach out to ISS to discuss the rationale underlying the negative vote recommendation. While these discussions might be helpful in determining whether a change in company practices or policies might cause ISS to reverse its negative recommendation, having such discussions in the midst of the proxy season may not always be possible. Once the proxy statement is filed, ISS analysts have discretion as to whether engagement with the company is necessary or appropriate, and they generally only engage with companies to clarify points on which they have questions. Moreover, ISS will not, in most cases, reverse a recommendation based solely on a conversation with the company because ISS bases its decisions on publicly available information. As such, reaching out to ISS before additional proxy soliciting materials are filed should be done only in limited circumstances.

- **Determine whether any changes to company practices or policies are feasible or desirable.** If it appears that a negative voting recommendation might be reversed if a company takes particular steps or adopts certain modifications, consider whether doing so would be appropriate for the company. For instance, if negative voting recommendations are based on company practice (e.g., the company has gross-ups), it may be simpler, and/or better from a governance perspective, to change the objectionable practices. Importantly, some changes will require more board involvement than others. When assessing whether to make any changes, companies should also consider tax rules (if, for example, they are amending employment agreements) and solicitation rules (if, for example, they are amending an equity plan that is up for approval at the annual meeting), among other things. Because ISS does not believe that company commitments to make changes in the future are relevant to its recommendations, ISS will, in most cases, only consider changes that a company will make immediately.

## Related Content

For an outline on how companies can prepare themselves for proxy voting recommendations from Institutional Shareholder Services (ISS), see

> [\*\*PREPARING FOR ISS PROXY VOTING RECOMMENDATIONS CHECKLIST\*\*](#)



**RESEARCH PATH:** [Capital Markets & Corporate Governance > Proxy Statement and Annual Meeting > Shareholder Activism > Checklists](#)

For guidance on how a company may exclude a shareholder proposal from its proxy materials, see

> [\*\*EXCLUDING SHAREHOLDER PROPOSALS AND SEEKING NO-ACTION LETTERS\*\*](#)



**RESEARCH PATH:** [Capital Markets & Corporate Governance > Proxy Statement and Annual Meeting > Shareholder Activism > Practice Notes](#)

For a detailed discussion on the distribution of proxy materials, see

> [\*\*MANAGING THE MAILING AND DELIVERY PROCESS FOR PROXY MATERIALS\*\*](#)



**RESEARCH PATH:** [Capital Markets & Corporate Governance > Proxy Statement and Annual Meeting > Mailing and Delivery of the Proxy Statement > Practice Notes](#)

- **If changes are made, publicly disclose these changes.** Any such changes should be communicated to shareholders by filing additional proxy materials on Form DEF14A (or a combination of both Form 8-K and DEF14A). Under the SEC rules, companies are not, in most circumstances, required to mail these supplemental materials to their shareholders. For a company that is not an SEC filer, a press release will be sufficient. Note that, as mentioned above, ISS generally will not change its voting recommendations within five business days of the company’s annual meeting. Therefore, any corrective action should be taken by the company (and any additional soliciting materials should be filed) as soon as possible after the receipt of a negative voting recommendation.
- **Promptly notify ISS.** According to ISS’s website, ISS does not review all documents as they are filed on the SEC’s website. Once the changes are disclosed publicly through an SEC filing, companies should notify ISS and send it a link to the filing. If the company discloses the changes and communicates them to ISS at least five business days



before the company's meeting, and if ISS determines that this new publicly available information warrants an update to its analysis consistent with its policy, ISS will issue a reversal of the earlier negative vote recommendation through a proxy alert. Any new information received less than five business days before the meeting will be discussed in an informational alert only if it is deemed to be material to the analysis, even if there is no change to ISS's voting recommendations.

ISS distributes the proxy alert to the same clients that received the original proxy report. It is typically overlaid on top of the original proxy report so that the original report, the updated information, and any vote recommendation change are contained in one document. Note that, according to the ISS's website, there may be circumstances, such as "egregious actions," where ISS would refuse to change its voting recommendation even if the company were to take the steps to cure the issues ISS identified in its report.

- **Contact top shareholders.** Even though ISS will alert investors to a corrective report, companies should not rely on investors seeing the revised report, especially if it is expected to be a tight vote. Therefore, companies

should alert their top shareholders themselves that a recommendation has been reversed.

Moreover, conducting outreach through calls or meetings with the voting personnel at the top institutional investors to make them aware of the additional soliciting materials might be helpful even if ISS does not ultimately reverse its voting recommendation.

#### *Glass Lewis*

Glass Lewis asks companies to notify them online (<http://www.glasslewis.com/report-error/>) if there is an error in a Glass Lewis proxy paper report. The submission should include (1) details on the issue, including meeting date, proposal number and title, page number in the report, and the full sentence in which the discrepancy appears; and (2) information as to precisely where within the company's public disclosure Glass Lewis can find and verify the correct information to revise its report. As with ISS, Glass Lewis bases its analysis strictly on publicly available information. If a company updates its proxy materials or notifies Glass Lewis of a purported factual error/omission, Glass Lewis will consider whether a revision to the report is appropriate. If Glass Lewis agrees that a revision to the report is appropriate, Glass Lewis will update its report to reflect new disclosure or the correction of an error. The

revised report will explain the nature of all revisions in a note in the report and notify clients via e-mail of the revised report, regardless of whether the update or revision affected Glass Lewis and/or clients' custom recommendations.

Glass Lewis typically will not discuss its policies or recommendations with issuers during the solicitation period (which begins on the date the notice of meeting is released and ends on the date of the meeting). However, Glass Lewis is willing to meet with companies during the solicitation period, if necessary, to discuss purported errors or omissions in its reports. In addition, if one of its analysts needs a clarification on a particular issue, Glass Lewis will contact the company or accept a request for a call during the solicitation period as long as the discussion is confined to publicly available information.

While it is rare for Glass Lewis to overturn a negative recommendation, if there is enough time before the meeting and the circumstances warrant a change under its voting policy, Glass Lewis may be willing to reverse a negative recommendation.

### *Governance*

Another area where companies frequently receive negative ISS recommendations is governance. Sometimes these recommendations are with respect to governance proposals; at other times, they are with respect to director elections, including the governance committee chair and/or other members of the board. For instance, in 2016 ISS recommended that shareholders withhold votes from the only member of one company's governance committee who was up for reelection that year. This was due to the company's decision to bundle two charter amendments (to declassify the board and to elect directors by majority vote) into a single voting item at its annual meeting and its proposed adoption of a majority vote standard for directors that did not include a provision for plurality voting in contested elections.

In subsequently filed additional soliciting materials, the company revised the proposal to amend its charter to require plurality voting in contested elections and to include a director resignation policy. ISS found this to be sufficient to mitigate shareholders' concerns and reversed its voting recommendation with respect to the governance committee member.





**... IT IS NOT EASY TO GET A  
PROXY ADVISORY FIRM TO REVERSE  
ITS VOTING RECOMMENDATION ONCE  
IT IS PUBLIC, EVEN WITH THE MOST  
WELL-WRITTEN ADDITIONAL PROXY  
SOLICITING MATERIALS.**

#### *Director Elections*

One of the most unpleasant situations a company sometimes has to deal with is receiving a negative voting recommendation with respect to one or more of its directors because the company did not realize that ISS would consider the director to be either on too many public boards or not independent under ISS guidelines (which, in some cases, are stricter than applicable listing exchange independence standards). However, depending on the director's and the company's circumstances, this, too, can be remedied.

For instance, one company had a director who was determined by the board to be independent under the New York Stock Exchange Listing Standards and who served on its nominating and corporate governance committee. ISS, however, determined that the director was not independent under its standards due to his former employment (more than three years before the proxy filing but within the previous five years) with what later became a subsidiary of the company.

After the company filed additional proxy soliciting materials disclosing that the director resigned from the nominating and governance committee, ISS reversed its recommendation with respect to this director.

#### *Accounting-Related Issues*

One of the easiest issues for a company to address is a lack of adequate disclosure. This can arise when a company discloses a material weakness in its internal controls. ISS has a specific policy that says that it will recommend votes against, or withhold votes from, members of the audit committee, and potentially the full board, if there are material weaknesses in internal controls identified in Sarbanes-Oxley Section 404 ([15 U.S.C. § 7262](#)) disclosures. ISS will examine "the severity, breadth, chronological sequence and duration, as well as the company's efforts at remediation or corrective actions, in determining whether withhold/against votes are warranted."

In one case, the company disclosed a material weakness in the previous two years and received a negative voting recommendation from ISS with respect to the company's audit committee members. ISS specifically noted that the

material weakness had persisted for two audit cycles and had not been remediated. The company filed additional proxy soliciting materials that detailed steps taken by its audit committee to remediate the material weakness and enhance internal controls, including that (1) three of the four material weaknesses had been remediated, while the fourth was in the process of being remediated; (2) the company needed additional time to be able to confirm that a sustainable, controlled process was fully in place; and (3) the company expected to complete the planned remedial actions during the then-current fiscal year. ISS deemed this information to be sufficient and reversed its voting recommendation.

#### **Market Outlook**

Although additional proxy soliciting materials will remain an important tool for companies responding to negative voting recommendations, shareholder engagement is expected to remain the real driver for filing additional soliciting materials. Filing additional soliciting materials shortly after a proxy statement is filed (even before proxy advisory firms release their voting recommendations) provides more time for companies to have conversations with their shareholders and for shareholders to conduct and complete whatever internal approvals are necessary to finalize their votes. Additional soliciting materials can be effective tools in shareholder engagement and in discussing a company's perspectives on a variety of issues or concerns that shareholders and proxy advisory firms may have. Given the importance of shareholder engagement and the ways that filing additional soliciting materials can facilitate engagement, additional soliciting materials are expected to continue to be an important part of responding to a negative voting recommendation. **L**

---

**Lori Zyskowski** is a partner in Gibson Dunn's New York office and a member of the Firm's Securities Regulation and Corporate Governance Practice Group. Ms. Zyskowski advises public companies and their boards of directors on corporate governance matters, securities disclosure and compliance issues, executive compensation practices, cybersecurity oversight, and shareholder engagement and activism matters. Ms. Zyskowski is a frequent speaker on governance, proxy, and securities disclosure panels and is very active in the corporate governance community. She is a member of the board of directors of the Society for Corporate Governance and served as Secretary to the board from 2011 to 2013.

---



**RESEARCH PATH:** [Capital Markets & Corporate](#)

[Governance > Market Trends > Corporate Governance &](#)

[Continuous Disclosure > Practice Notes](#)

# RELX Unveils Content Hub Spotlighting **United Nations'** **Sustainable Development Goals**

**RELX GROUP HAS LAUNCHED A DEDICATED NEWS AND** information resource in support of the 17 Sustainable Development Goals (SDGs) promulgated by the United Nations in its 2030 Agenda for Sustainable Development.

The [RELX Group SDG Resource Centre](#) features content aimed at increasing awareness and implementation of the SDGs, which were adopted by 193 states at the United Nations in September 2015. The interactive platform was announced at Inspiration Day, a forum hosted in London by RELX Group, the UN Global Compact UK, the Business and Sustainable Development Commission, and the Responsible Media Forum.

"Businesses can make a real difference by harnessing their expertise to advance the SDGs," said Dr. Márcia Balisciano, Director of Corporate Responsibility at RELX Group. "This is the aim of our SDG Resource Centre."

The Resource Centre contains articles, reports, tools, webinars, videos, legal practical guidance, and discussion groups on science, law, business, and events from across RELX Group and its divisions. Content is tagged by relevant topic and region and grouped according to the specific SDG addressed.

Examples of content featured in the SDG Resource Centre include:

The [Sustainability Science in a Global Landscape](#) report (exploring the state of science underpinning the SDGs) from Elsevier, which plays an important role in advancing human welfare and economic progress through its science and health information.

The [Rule of Law Impact Tracker](#) developed by LexisNexis Legal & Professional and the World Justice Project, helping to strengthen SDG 16 focused on peace and justice.

Information from [Proagrica](#) which combines data and analytics to improve agricultural yields and ensure sustainable land use, based on the open source [HPCC Systems](#) technology from Risk & Business Analytics.

Details on events providing platforms for supporting the SDGs such as Reed Exhibitions' [World Future Energy Summit](#) focused on affordable and clean energy and [World Travel Market](#) dedicated to sustainable tourism.

The UN's 2030 Agenda is aimed at ending poverty, protecting the planet, and ensuring peace and prosperity for all people across the globe by way of a global partnership focused in particular on the needs of the poorest and most vulnerable populations.

The 17 SDGs are:

- No Poverty
- Zero Hunger
- Good Health and Well-Being
- Quality Education
- Gender Equality
- Clean Water and Sanitation
- Affordable and Clean Energy
- Decent Work and Economic Growth
- Industry, Innovation and Infrastructure
- Reduced Inequalities
- Sustainable Cities and Communities
- Responsible Consumption and Production
- Climate Action
- Life Below Water
- Life on Land
- Peace, Justice and Strong Institutions
- Partnerships for the Goals

RELX Group is a global provider of information and analytics for professional and business customers across industries. The Group serves customers in more than 180 countries and has offices in about 40 countries. It employs approximately 30,000 people of whom almost half are in North America. RELX PLC is a London listed holding company which owns 52.9% of RELX Group. RELX NV is an Amsterdam listed holding company which owns 47.1% of RELX Group. The shares are traded on the London, Amsterdam, and New York Stock Exchanges using the following ticker symbols: London: REL; Amsterdam: REN; New York: RELX and RENX. The total market capitalization is approximately \$43 billion.



LexisNexis®

Public Records  
on Lexis Advance®

NO ONE ELSE COMES CLOSE

65

BILLION  
PUBLIC RECORDS

INCLUDING DRIVER'S LICENSE RECORDS FROM  
3X AS MANY STATES\*



VOTED BEST ONLINE PUBLIC RECORDS  
RESEARCH PROVIDER



Start your free trial today

LEXISNEXIS.COM/65BILLION  
800.628.3612



682 MILLION  
EMAIL ADDRESSES



2.7 BILLION  
BUSINESS CONTACTS



272 MILLION  
CELL PHONE NUMBERS



1.1 BILLION  
VEHICLE TITLES

\*As compared to Westlaw®. Comparison data based on information available as of October 2016.  
LexisNexis, Lexis Advance and the Knowledge Burst logo are registered trademarks of RELX Inc. Westlaw is a registered trademark of West Publishing Corporation.  
Other products or services may be trademarks or registered trademarks of their respective companies. © 2017 LexisNexis. BMH00722-2 0417





LexisNexis®

Lexis Practice Advisor®

# START HERE TO GET IT RIGHT

Get off on the right foot in your matters with  
effortless navigation to expert guidance.

Try Lexis Practice Advisor® today

[LEXISNEXIS.COM/PRACTICE-ADVISOR](https://www.lexisnexis.com/practice-advisor)

800.628.3612

650+

ATTORNEY  
AUTHORS

91%

ATTORNEY AUTHORS  
CURRENTLY PRACTICING

260+

CONTRIBUTING  
LAW FIRMS

2x

MORE PRACTICING  
ATTORNEY AUTHORS\*

\*As compared to Thomson Reuters Practical Law network. Comparison data based on information available as of June 2017.

LexisNexis, Lexis Practice Advisor and the Knowledge Burst logo are registered trademarks of RELX Inc. Westlaw is a registered trademark of West Publishing Corporation. © 2017 LexisNexis. PA00211-0 0817