"Managing Enterprise-Wide Risks: The Intersection of ERM & Legal"

Thursday, March 21, 2023

Course Materials

“Managing Enterprise-Wide Risks: The Intersection of ERM & Legal”

Tuesday, March 21, 2023

2 to 3 p.m. Eastern [archive and transcript to follow]

The SEC, investors and Delaware courts have been heavily focused in recent years on how companies oversee enterprise risk management (ERM). This attention has increased the pressure on senior executives and boards of directors to find new ways to enhance and update their ERM programs and disclosures, and legal departments are playing a critical role in this process.

Join these panelists:

- **Stephanie Bignon**, Associate General Counsel and Assistant Secretary, WestRock Company
- **Ming-Hsuan Elders**, Senior Counsel, American Express
- **J.T. Ho**, Partner and Co-leader of Orrick's Public Companies and ESG Practice
- **Jeff Levinson**, Senior Vice President and General Counsel, NetScout
- **Derek Windham**, Deputy General Counsel for Corporate and Securities, Tesla

Among other topics, this webcast will cover:

- How ERM Differs From Traditional Risk Management
- The Issues to Consider When Implementing an ERM Program
- The Board and Management's Role in Enterprise Risk Management, and *Caremark* Considerations
- The Growing Role of the Legal Department in Enterprise Risk Management
- The SEC's Recent Focus on Enterprise Risk Management Disclosures
- The Relationship Between ERM and ESG

“Managing Enterprise-Wide Risks: The Intersection of ERM & Legal”

Course Outline / Notes

1. How ERM Differs From Traditional Risk Management

2. The Issues to Consider When Implementing an ERM Program

3. The Board and Management’s Role in Enterprise Risk Management, and *Caremark* Considerations

4. The Growing Role of the Legal Department in Enterprise Risk Management

5. The SEC’s Recent Focus on Enterprise Risk Management Disclosures

6. The Relationship Between ERM and ESG

“Managing Enterprise-Wide Risks: The Intersection of ERM & Legal”

Table of Contents — Course Materials

Checklist: Risk Assessment – Evaluation of Existing Practices

By Jeff Kaplan, Kaplan & Walker

While there are many standards for evaluating your existing risk assessment practices, the best is the simplest: does the process actually produce results that will help the company have effective Compliance & Ethics (C&E) program elements? In self assessing against this standard, a company might ask whether its current process helps the company do the following:

1. Determine whether additional C&E policies are needed for any given part of the company (e.g., business or geographical unit) on any given topic, or the extent to which such policies need to be revised.

2. Develop company-specific examples or Q&A that can help make a code of conduct less abstract.

3. Determine whether any additional C&E communications (training or other) should be targeted at any particular part of the company on any given topic.

4. Develop/enhance C&E audit protocols, monitoring tools and other approaches to "checking" on both an enterprise-wide and local "level."

5. Identify C&E risks for which additional controls are warranted, such as pre-approvals by management or staff for specified (high-risk) activities.

6. Establish additional C&E oversight/reporting responsibilities for high-risk areas.

7. Add C&E components to job descriptions, performance-evaluation criteria or business unit plans in a risk-based way.

8. Determine whether incentives in any part of the Company pose an undue risk from a C&E perspective.

9. Assess where and the extent to which aspects of a C&E program should apply to contractors, vendors and other third parties.

10. Develop metrics for measuring the effectiveness of C&E efforts directed at individual areas of risk. (Note: for many companies, metrics are still purely a matter of overall program process, e.g., number of calls to the "Concerns Line")

11. Identify true ethics, as well as compliance, issues that the program should address.

12. Identify cultural C&E risks, such as lack of employee identification with the company or its mission, short-term thinking or other "moral hazard" related risks.

13. Provide a stronger foundation for the program oversight by the Board.

14. Provide a basis for future/"evergreen" risk assessments.

Checklist: Risk Factors – Determining Risks

By TheCorporateCounsel.net

Companies are required to provide a description of the risk factors that make their offering speculative or risky in their registration statements. Additionally, this "risk factor" disclosure is required for 1934 Act periodic reports pursuant to Item 1A of Part I of Form 10-K and Item 1A of Part II of Form 10-Q. These disclosure requirements are based on Item 105 of Regulation S-K.

But risk factors aren't just a disclosure requirement – they're a benefit. When done right, risk factor disclosure can be a formidable defense to securities fraud claims. In addition, the benefits of a well-crafted risk factors go beyond liability protection. Good risk factor disclosure can be every bit as valuable an investor relations tool as it can be as liability insurance. After all, being able to say, "I told you so" to investors means "never having to say I'm sorry."

Here are some considerations when determining which risk factors to include in your disclosure:

1. **Infinite Risk Factors Topics:** A "risk factor" is anything that makes an investment in the company speculative or risky. In registration statements, risk factors often include information about the company's lack of an operating history, lack of profitable operations in recent periods, financial position, business or a lack of a market for the company's securities. As discussed more below, the SEC strongly discourages the use of "generic" risk factors that could apply to any company or any offering – so you need to tailor the disclosure to your specific situation.

2. **Number of Risk Factors:** There's no minimum – or maximum – number of risk factors that a company can or should disclose. The number will depend on a company's own circumstances, the disclosure document, the company's risk disclosure approach – and perhaps also on the custom of the disclosure drafters.

   Many variables impact the number of risks – *e.g.*, company size, industry, maturity, geographic reach, whether and how risks are "bundled," disclosure philosophy, etc. As a result, in practice, there are some companies with far more – and far fewer.

3. **Risk Factors Must Be Concise:** Although Item 105 doesn't expressly limit the number of risk factors that a company can include in its registration statement or report, it does require risk factor disclosure to be concise. If the section is

longer than 15 pages in total, Item 105 requires a concise, bulleted or numbered list in the forepart of the prospectus or annual report that summarizes the principal risk factors. That summary has to be 2 pages or shorter. In practice, the requirement to include a summary means that most companies try to keep their risk factor disclosure under 15 pages in length, which could limit the number of risk factors that are included.

4. **Categorize Risk Factors:** When identifying risk factors, bear in mind that Item 105 of Regulation S-K requires that your risk factors be logically organized, with relevant headings. The SEC believes that a well-organized risk factor discussion helps investors make more efficient decisions – for example, risks that are more likely or that could have a significant negative impact should be more prominent. When Corp Fin published Staff Legal Bulletin No. 7A regarding its plain English rule in mid-1999, it noted that risk factors generally fall into the following three broad categories, and instructed companies to link each of their stated risk factors with the applicable category:

   - **Industry Risk** – These are risks that the company faces because of the industry it is in. For example, real estate investment trusts run the risk that – despite due diligence – they will acquire properties with major environmental issues.

   - **Company Risk** – These risks are specific to the company. For example, a REIT may actually own properties with significant environmental issues, and face significant clean-up expenses.

   - **Investment Risk** – These are risks that are specifically associated with a security. For example, in a debt offering, the debt being offered may be the most junior subordinated debt of the company.

   Some companies organize their risks under these specific headings but they're not required categories. We don't think companies need to use these particular headings but you do need to use relevant headings to group your risk factors.

5. **Subcaption Each Risk Factor:** Item 105 also requires each risk factor to be set forth under a subcaption that adequately describes the risk. Just like the full risk factor, the subcaption should be tailored to your company.

6. **Put Any Generic Risk Factors Under "General Risk Factors" Caption:** Item 105 discourages disclosure of generic risk factors that could apply to any company or any offering. To the extent a company discloses generic risk factors, Item 105 says that it should include them at the end of the risk factor

section under a separate caption, “General Risk Factors.” Most companies try to avoid this.

7. **Balance Low Probability Risks With High Magnitude Risks:** Identifying risk factors for disclosure purposes sometimes can be challenging, as the SEC is seeking disclosure of all risks that the company believes are “material” at the time of disclosure. Determining materiality entails consideration of both the magnitude & probability of occurrence of any particular risk. Risk factors should be chosen with this in mind so that the most significant and material risks are disclosed.

8. **Interplay With Risk Management Program:** Most companies – and virtually all large companies – have a formal risk management/insurance department. These risk management programs also typically include some degree of cross-functional collaboration with people outside of the risk management group – *e.g.,* executives, finance, legal and compliance.

   This means that risk management procedures are easily adaptable to permit those responsible for disclosure to assess the advisability of disclosure of those risks. The legal & financial reporting teams can use their involvement in the risk assessment process to generate the type of information they need in order to develop strong disclosure controls & procedures around the "Risk Factors" section.

   For some companies – mainly smaller ones – the risk management infrastructure may not be as robust. As a result, it's going to require more work for these companies to build a systematic process for identifying risk factors. The good news is that the payoff is large, because not only will investing in improving disclosure controls & procedures in this area enhance their ability to generate more meaningful and tailored risk factor disclosure, it will also enhance the overall risk management program itself.

9. **Benchmark Against Peers:** Particularly for risk factors associated with industry risk, it’s important to look at the SEC filings of the companies in your peer group to see what types of risk factors they disclose – as well as Corp Fin comment letters and public remarks to assess the latest areas of Staff concern. This can help provide ideas for areas that your risk factors potentially should cover, as well as help ensure that your disclosure isn’t an “outlier” for liability purposes. You shouldn’t conform your risk factors disclosure to another company’s disclosure simply for the sake of uniformity.

The risk factor disclosure of other companies in the same industry should prompt thought and discussion internally as to whether – and to what extent – risks that you haven't identified (or haven't identified as significant enough for disclosure purposes) may apply to your company so that inclusion of such risks, tailored to your company makes sense.

It's also a good idea to benchmark your risk factors against companies not in your industry, perhaps looking at the Form 10-Ks filed by companies with a reputation for good disclosure practices.

10. **Review Board & Committee Minutes:** The board's increasing role in oversight of the risk management function means that a lot of risk-related issues percolate up to the board (or its committees). Reviewing board & committee minutes is indispensable to getting a good grasp on the key risks the company is facing.

    What's more, reading the minutes is often a quick & dirty way to prioritize those risks. Chances are if something's made it to the boardroom, a lot of people have already decided that it's pretty important.

    When you review board & committee minutes, don't limit yourself to matters specifically identified as involving risk management. There may be substantive matters addressed in other settings that could have important implications for risk factor disclosures. For instance, there may be developments in the business or contingencies that are addressed in the ordinary course of the meeting that might flag new risks – or suggest that previously identified risks might merit higher priority as disclosure items.

11. **Analyst Reports & Investor Feedback:** Reports issued by securities analysts on your company and similar materials often contain a wealth of information concerning each analyst's views on the significant risks that face your company and its industry. They may – or may not – align with your internal risk assessments, but they'll sure play a big role for your shareholders.

    Along the same lines, part of the process of developing your risk factors should include reaching out to the company's investor relations group. The IR group is uniquely positioned to share the areas of potential risk that investors have been focusing on, as well as the responses to risk-related questions that have been provided by members of senior management.

12. **Trade Publications:** Publications, websites and other media reports on your industry can also provide helpful information on the risks that your company

and its competitors face. Like analyst reports on the industry, these publications may aid in determining what risks you share in common with your peers – but perhaps more importantly, they may help you identify areas of divergence thatshould be highlighted in your own disclosures.

13. **Don't Include Risks Applicable to Any Company:** Item 105 specifically states that risks that apply to any company (or any offering) shouldn't be disclosed as a risk factor. Part of the reason Item 105 requires a bullet-point summary if the risk factor section exceeds 15 pages is to discourage inclusion of generic information that is less meaningful to investors because it could apply to any investment.

    While easy to understand in concept, this actually is pretty difficult to apply in practice because many of the risks that apply across the board to all companies might impact your company in a unique way (*e.g.*, the scope of operations or locations of major facilities may provide your company with particularly significant exposure to a financial crisis or a specific disaster event). In addition, these types of broad risks often may be among the most material.

    In many cases, companies err on the side of caution and disclose these types of broad risks anyway. Companies that take this approach should consider whether this obscures the more relevant and material risks that are disclosed.

    Inclusion of risk factors that could apply to any company or any offering without a clear explanation as to how they apply specifically to your company have frequently elicited Corp Fin comments citing Item 105 and requesting that inclusion of such risk factors be re-evaluated or tailored. Therefore, if these types of risk factor are disclosed, companies should avoid generic risk factor disclosure and illustrate how the risk specifically applies to its specific facts and circumstances.

    To the extent a company discloses generic risk factors, Item 105 requires them to be grouped together at the end of the risk factor section under a separate caption, "General Risk Factors."

    Court cases illustrate that disclosure of broad risk factors that aren't specifically tailored to the company's circumstances typically won't protect against liability. If a risk is truly general and broad – rather than include it as a risk factor – consider whether it might fit better in other sections of the Form 10-K, like the MD&A, Legal Proceedings or Regulation sections.

14. **Macro Trends May Be Appropriate:** Risk factors relating to general economic conditions or other macro trends or events may be appropriate to disclose. For example, during the financial crisis in 2008 & 2009, many companies disclosed risk factors about the economy. That was appropriate as it would have been difficult to provide adequate disclosure without addressing general macro-economic trends and the adverse financing conditions arising from that intense credit crunch. More recently, many companies have added risk factors to address cybersecurity & privacy risks, climate change, Brexit, LIBOR and the COVID-19 pandemic – make sure to refresh your risk factors on these topics. For instance, you'll want to revisit your COVID-19 risk factor as the company is more able to gauge the actual risks and impact to the business at the end of 2021 vs. in early 2020. The key in disclosing such risks is to include specific disclosure of why & how the company would be impacted (which varied by, *e.g.,* industry, geographic reach, growth strategy, stage of maturation, liquidity position, etc.).

    As noted in the September-October 2008 issue of *The Corporate Counsel*, the SEC addressed macro disclosure head-on in an amicus brief submitted in Kapps v. Torch Offshore, No. 0330227 (Fifth Circuit, June 2003), available under "Amicus/Friend of Court Briefs" in the Litigation section on sec.gov.

    The SEC's brief argues that the District Court was incorrect when it held the "federal securities laws don't impose a duty on issuers to disclose industry-wide trends or publicly available information." While the focus here was on Item 303 (MD&A) disclosure, the Risk Factors section is intended to be a summary of more detailed risk discussion contained elsewhere in the document, such as in the MD&A.

15. **Tailor Macro Trends:** When drafting risk factors relating to general economic conditions or other macro trends or events, one concern is an "overemphasis" on external economic, market and credit conditions as a source for adverse business trends specific to the company. In some cases, this overemphasis may be potentially misleading, particularly if the company doesn't provide adequate disclosure about how the macro trend or event specifically impacts its own operations.

    The crux of the concern is that it is much easier to blame the economy or other macro factors for disappointing results than to criticize one's own business – *i.e.,* to explain why & how company-specific factors or circumstances cause particular concern as to the potential impact to the company of the stated risk. Simply citing a macro trend or event without tailoring it to the company doesn't

serve the purpose of including the risk factor. For example, Corp Fin's 2011 guidance on cybersecurity risks makes it clear that risk factors must be tailored to the company. Also see the SEC's 2018 interpretive release – Release No. 33-10459 and its settlement with Altaba (f/k/a Yahoo!) for alleged disclosure shortcomings.

In addition, for the same reason (*i.e.,* criticizing one's own business is difficult),there can be a tendency to over-emphasize macro trends and events outside of the company's control and even industry-wide factors (which still must be tied to company-specific circumstances, as industry-wide factors may, and often do,affect individual companies differently), and under-emphasize company- specific risks (*e.g.*, gaps in upper management, current material litigation or investigatory proceedings, competitive challenges unique to the company) that may adversely impact the company's business, financial condition and results of operations.

So we think there should be some balance in discussing company-specific, industry-wide and macro-economic trends and uncertainties and other risks – the potential impact of each which must be tailored to the company based on its specific facts & circumstances.

16. **Common Risk Factors:** Here are common risk factors used in both '34 Act & '33 Act filings:

- Failure to Compete Successfully
- Trading Market May Not Develop/Potential Share Price Volatility
- Dependence on Management Team
- Difficulty Raising Capital/Insufficient Funding
- General Economic/Consumer Spending Conditions
- Failure to Protect Intellectual Property Rights
- Negative Impact of Changes in Regulations/Policies
- Dividends May Never Be Paid
- Principal Shareholders/Management Will Have Significant Control
- Anti-Takeover Provisions May Prevent a Merger/Acquisition

- Cybersecurity risks

Here are some additional risk factors that are often used:

- History of Losses/No Revenue
- Operational Disruptions
- Potential/Current Litigation/Claims
- Dilution in Ownership Due to Future Share Issuances/Conversions
- Failure to Maintain Effective Internal Controls
- Failure to Manage Growth / Expansion Costs
- Integration Challenges from Merger/Acquisition
- Impact of International Regulations, Political Climate and Economic Conditions

For more information, see our "Risk Factors Disclosure Handbook" - posted along with other resources in the "Risk Factors" Practice Area on TheCorporateCounsel.net.

Checklist: Risk Management - Cybersecurity

By TheCorporateCounsel.net

1. Risks & Consequences Justify Program: The expansive risks associated with cybersecurity - and increasing number and magnitude of cyber incidents and threats - call for development and implementation of a robust cybersecurity program to help prevent and mitigate the potential for breaches and associated consequences. Consequences of cybersecurity incidents vary significantly by type and magnitude, but, on average, cost millions of dollars per breach (according to studies from the Ponemon Institute and others). Damages may include:

- Reputational harm
- Lost revenues due to increased customer turnover, reduction in new customer rate, diminished goodwill
- Lost revenues due to unauthorized use of proprietary information
- Business interruption
- Management distraction
- Customer lock-outs from company networks and services
- Violations of privacy laws for disclosure of personal information
- Violations of disclosure requirements if breaches result in material financial or business consequences
- Law enforcement investigations - FBI, Secret Service, ICE, ATF, US Postal Inspection Service
- Litigation
- FTC enforcement for breaches resulting in compromised customer information
- Remediation costs, e.g., liability for stolen assets/information, repairing system damage, offering incentives to customers/business partners to maintain relationships

- Increased regulatory scrutiny about adequacy of prevention & mitigation measures and cyber disclosures

- Stock price decline & loss of investor confidence

- Increased protection costs following a breach, e.g., organizational changes, deploying additional personnel & protection technologies, employee training, engaging 3rd party experts

2. <u>Cybersecurity Program Building Blocks:</u> Although each company faces unique cyber risks that should shape its cybersecurity program, any cybersecurity program should address these elements:

<u>Cyber threat defense & mitigation:</u>

- Identification of major cybersecurity risks, including risks associated with vendors and other 3rd party service providers and "insider" threats

- Risk prioritization based on identification of the most sensitive and critical information and breach implications

- Identification/development of associated detective and risk management & mitigation measures

- Documentation & periodic testing, and internal auditing, of program components

<u>Threat detection, intelligence & analysis:</u>

- Forensic & investigative activities

- Assessment & audit services

<u>Disclosure controls and internal controls:</u>

- Framework & training that explains when and what types of incidents should be elevated internally to assess SEC reporting obligations (e.g. AICPA SOC for Cybersecurity)

- Controls & training to allow employees to protect company assets from cyber-threats (e.g. fraudulent funding requests, as outlined in the SEC's 2018 Section 21(a) Report on Internal Controls)

Cyber incident response: See our separate checklist addressing response plans

Incident remediation & recovery:

- Help desk activities & other actions to handle inbound communications
- Special investigations
- Restoration of systems
- Legal & PR services
- Customer discounts
- Customer identity protection, credit report monitoring services
- Issuance of new customer accounts or cards
- Regulatory interventions & investigations
- Elimination of weaknesses evidenced by the breach & identification of other necessary security improvements to avoid recurrence

Additional overarching considerations applicable to programs include:

- Executive responsibility and accountability clearly defined
- Representation from & coordination among key departments including IT, HR, Legal, Compliance, business units
- Board periodic review & oversight
- Employee education & training about cyber risks, prevention, detection & abatement
- Adequacy of budget & staffing
- Use of internal vs. external resources
- Existence & adequacy (scope & amount) of insurance coverage
- Periodic reporting to senior management from responsible personnel (e.g., IT, outside risk assessment professionals) about cybersecurity risks & risk management

- Management periodic reporting to the board about cyber risks & risk management

- Review & update of program annually and upon identification of threats, occurrence of incidents

- Monitoring of technological, industry & public policy developments on cybersecurity risks & remedies

- Making proper cybersecurity & cyber incident disclosure in accordance with SEC regulations and guidance

3. <u>Board Oversight Considerations:</u> The board should - and commonly does - oversee cybersecurity risk as part of its broader risk management oversight function.

Based on an abundance of survey data, responsibility for risk oversight is most frequently retained by the full board or assigned to the audit committee (although it is also fairly common to allocate responsibilities across all board committees). However, due to the audit committee's declining ability to oversee all of the company's major risks in addition to carrying out its core responsibilities, boards are increasingly reallocating or rebalancing risk responsibilities - or creating a new committee - to address specific risks such as cybersecurity.

Board oversight considerations include:

- Ensuring there is a clear allocation of responsibilities among the full board and its committees for overseeing cyber risks

- Director education about cybersecurity to bolster the board's oversight (see our separate director education checklist)

- External support – many boards use outside consultants to advise them on IT strategy, opportunities and risk

- Working with senior management to understand the company's cybersecurity risks - including potential likelihood, frequency & severity of cyber-attacks and data breaches - and risk tolerance

- Reviewing with management - and ensuring the adequacy of - the company's cyber risk management practices in the context of the risk profile

- Ensuring existence & adequacy of insurance coverage for losses associated with data breaches

- Ensuring adequacy of the annual cyber risk management budget, including funds to retain outside consultants if appropriate

- Ensuring development & adequacy of an incident response plan and adequacy of resources to respond to a breach

- Audit committee's use of internal audit to review controls pertaining to cybersecurity & evaluate cybersecurity weaknesses as part of its risk-based audit plan

- Audit committee's use of outside auditor for information & resources on cybersecurity issues (including security controls)

- Ensuring offshore operations, processes & data are subject to the same protections and contingency plans as those put in place domestically

- Addressing gaps in necessary expertise & experience in the board's composition – e.g. adding one or more directors with first-hand IT experience that is relevant to the company's specific risks and opportunities

- Periodic reporting from senior management (increasingly, a CIO) and/or responsible personnel (e.g., IT managers) about cybersecurity risks, risk management and threats

- Engaging periodic third-party assessments of company's cybersecurity program

- Understanding the company's cybersecurity & cyber incident disclosure, and associated SEC regulations and guidance

- Awareness of major institutional investor and proxy advisor expectations about board oversight

At the board committee level, here are some ideas:

- Include at least one director with an information technology background on the committee

- Provide written report from Chief Security/Information Officer at each regularly scheduled committee meeting, which could include actions that the company is taking to remain up-to-date on threats and protective measures, data breach incidents, if any, improvements underway, etc.

- Provide executive summary of data protection plan to committee at least annually

- At least twice a year, have the Chief Security/Information Officer available to answer live questions from the committee

- At least once a year, have outside counsel and outside IT consultant available to answer live questions from the committee.

See our separate checklists addressing board risk oversight – posted in our "Risk Management" Practice Area on TheCorporateCounsel.net – and the numerous checklists & other resources posted in the "Cybersecurity" Practice Area on TheCorporateCounsel.net.

Checklist: Risk Factors – Drafting Tips

By TheCorporateCounsel.net

Companies are required to provide a description of the risk factors that make their offering speculative or risky in their registration statements. Additionally, this "risk factor" disclosure is required for 1934 Act periodic reports pursuant to Item 1A of Part I of Form 10-K and Item 1A of Part II of Form 10-Q. These disclosure requirements are based on Item 105 of Regulation S-K.

But risk factors aren't just a disclosure requirement – they're a benefit. When done right, risk factor disclosure can be a formidable defense to securities fraud claims. In addition, the benefits of a well-crafted risk factors go beyond liability protection. Good risk factor disclosure can be every bit as valuable an investor relations tool as it can be as liability insurance. After all, being able to say "I told you so" to investors means "never having to say I'm sorry."

Here are some risk factor drafting tips for your consideration:

1. **Use Descriptive Captions:** Captions must adequately describe risk factors. More so than other captions used in SEC filings, the captions for risk factors must be considered carefully. Item 105 specifically states: "each risk factor should be set forth under a subcaption that adequately describes the risk." Each caption should be in plain English with an active voice, everyday language, etc.

   It's not uncommon for a caption to be more than a few words – often the caption will be longer to ensure it captures the essence of the risk. In fact, the Corp Fin Staff has specifically commented on the inadequacy of risk factor captions when they fail to be specific or to adequately describe the risk discussed in the accompanying text.

2. **Use Plain English:** Even though it's common sense to draft risk factors so investors can understand them – particularly since they serve to protect the company – pursuant to Item 105 of Regulation S-K, the Risk factors disclosure must be drafted in plain English in accordance with Securities Act Rule 421(d) of Regulation C.

   Here's an excerpt from Staff Legal Bulletin No. 7A addressing what the Corp Fin Staff is looking for:

   > Registrants must use plain English writing principles in the

organization, language, and design of the front & back cover pages, the summary, and the risk factors section. Also, when drafting the language in these parts of the prospectus, registrants must substantially comply with these plain English principles:

- Short sentences;
- Definite, concrete everyday language;
- Active voice;
- Tabular presentation of complex information;
- No legal jargon; and
- No multiple negatives.

In designing these and other parts of the prospectus, registrants may include pictures, logos, charts, graphs, or other design elements so long as the design isn't misleading and the required information is clear.

The SEC made clear in footnote 593 of the Securities Act Reform adopting release in 2005 that risk factor disclosure in 10-Ks must comply with Rule 421(d) – the plain English rule – just like they were historically required to be drafted if the company wanted to incorporate them by reference into a registration statement.

3. **Summary of Risk Factors Required if Risk Factors Exceed 15 Pages:** When a company's risk factor section exceeds 15 pages, Item 105 of Regulation S-K requires a summary risk factor disclosure of no more than two pages. The summary is intended to improve readability. Item 105 requires that a risk factor summary be a series of concise, bulleted or numbered statements. Although Corp Fin Staff haven't provided authoritative guidance about the risk factor summary, they have indirectly indicated that Corp Fin wouldn't object to a forward-looking statement section serving as the risk factor summary, provided the forward-looking statement section otherwise satisfies the requirements of an Item 105 risk factor summary.

4. **Group Risk Factors Under Relevant Headings and Organize to Best Present Material Risks:** Given the purpose of disclosing risk factors, it naturally follows that companies should highlight those risk factors that

appear to pose the greatest risk. Risk factors need to be grouped under relevant headings and then organized in a way that you determine most effectively presents the material risks that make an investment in your company's securities speculative or risky.

Bear in mind that "magnitude" doesn't necessarily equate to level of materiality (e.g., if the probability of occurrence is virtually nil, the risk may be ranked lower even if the potential magnitude is significant). When organizing risk factors according to various categories and under relevant headings, companies should order the risk factors within each category according to priority.

Although the SEC doesn't specifically require prioritization of risk factors, it's a best practice. This serves to inform investors which risks have the greatest potential consequences (which also serves to protect the company in the event such risks come to pass). After all, nobody is better situated than management to help investors understand the significance of particular risks. Note that Item 3.D of Form 20-F states: "Companies are encouraged, but not required, to list the risk factors in the order of their priority to the company."

5. **Reorder As Materiality Changes:** A review for potential updates to the risk factor section (e.g., updates to existing risk factors, new risk factors, etc.) should be conducted at least quarterly in connection with the Form 10-Q, if not more frequently.

   Each time a company updates its risk factor disclosure an analysis of whether the nature or magnitude of a risk has changed should be conducted – and based on that review & analysis – there should be a reordering of the risk factors. Reordering should accompany any changes in the risk factor language, as appropriate.

6. **Organize By Common Category/Theme:** Item 105 requires you're your risk factors be "organized logically with relevant headings." The SEC believes that a well-organized risk factor discussion helps investors make more efficient decisions – for example, risks that are more likely or that could have a significant negative impact should be more prominent. Companies often address company-specific risks first, followed by industry-specific risks and then risks related to their common stock or other securities.

7. **Put Any Generic Risk Factors Under "General Risk Factors" Caption:** Item 105 discourages disclosure of generic risk factors that could apply to any company or any offering. To the extent a company discloses generic risk

factors, Item 105 says that it should include them at the end of the risk factor section under a separate caption, "General Risk Factors." Most companies try to avoid this.

8. **Be Specific About Downsides:** The Corp Fin Staff takes seriously Item 105's injunction to avoid disclosing risks that could apply to any company— and often issues comments telling companies that appear to be including generic risk factors to either particularize those risk factors to their own company or to delete them. We think that the most common reason for a comment like this is a failure to be specific about the consequences to the company that could come to pass if the risk warned about transpired.

   For example, it's one thing to say that an increase in interest rates could have a material adverse effect on the company's financial condition—the Staff's likely reaction is going to be something along the lines of "yeah, you and everybody with a credit card." However, if your disclosure about a macroeconomic event like a change in interest rates focuses on specific consequences to your business resulting from the nature of your capital structure, degree of leverage or some other company-specific issue, we believe you are much less likely to draw this kind of comment.

9. **Don't Use Mitigating Language:** When drafting risk factors, don't explain risks away or otherwise include mitigating factors. Although tempting to do so, don't try to list all the reasons why a risk explained in a risk factor isn't a real risk or may be minimized. That isn't the purpose of the Risk Factor section.

   That's something more for the MD&A or Business section. Plus, if the countervailing considerations are that noteworthy, consider whether the risk might not be sufficiently significant to belong in the risk factors disclosure.

   Furthermore, effectively minimizing or eliminating the risk with countervailing considerations reduces the protection otherwise afforded to the company by the disclosure. This is a common area of comment by the Corp Fin Staff if they spot "caveats."

10. **Don't Generalize If Risk Has Materialized:** If a risk has started to materialize, the risk factor shouldn't just be discussed generally, conceptually or theoretically—it should describe specifically what has already occurred and then set forth the risks going forward.

11. **Tie to Other Sections of Disclosure Document:** Not only might it be useful

for risk factors to cross-reference to forward-looking information existing in the same disclosure document (as part of the safe harbor mechanics), it's wise to carefully read through the periodic report – particularly the MD&A and Business section – and see if there are any known or unknown trends, uncertainties, key business strategies, etc. for which specific risk factor disclosure may be warranted, keeping in mind that the Risk Factor section is intended to disclose all material risks at the time of publication and to summarize those risks discussed in greater detail elsewhere in the document.

12. **Draft Risk Factors Last:** Along those same lines, don't make the Risk Factors section the first thing you draft. Instead, make it the last. Focusing on updating your risk factors after you've had a chance to prepare & review the other disclosures in the document will help you do a couple of things.

    First, it may shake out additional risk factors that should be included. For example, if you find yourself with interesting MD&A disclosure about known trends, you may want to also flag the key uncertainties in your risk factors. Along the same lines, if you've got some contingencies flagged in a financial statement footnote, you may want to address them in your risk factors too.

    The other thing that this process will do is help you make sure that the disclosure in various parts of the document appropriately elaborates on the information that's been flagged in the risk factors section. The Corp Fin Staff has frequently commented that risk factors should be a more concise summary of risks discussed in full elsewhere in the company's filings such as in the MD&A or Business sections.

    This means that your substantive disclosures should be informed by the risk factors you've identified—and if you cross reference another part of the document in your discussion of a particular risk factor, you want to make sure that additional meaningful information about the substantive matters giving rise to the risk is included there.

13. **Review Corp Fin Plain English Samples:** Back when the SEC's plain English rule was adopted in 1998, the Corp Fin Staff issued two Staff Legal Bulletins to help companies comply with new Rule 421(d). At the time, the Corp Fin Staff thought Item 105 was the least understood of the plain English requirements – so they provided sample risk factor disclosures and subheadings in SEC Staff Legal Bulletin No. 7A. Even though these samples – in a nifty "before" & "after" chart—are over a decade old, they still are useful to those not used to drafting in a plain English style.

14. **Review Corp Fin Comments:** The Corp Fin Staff frequently issues comments on risk factors when it reviews periodic reports (and registration statements). You may want to review the comment letters received by companies in your industry group by conducting a search on the SEC's Edgar database (or using commercial services that allow for greater search functionality). In addition, Staff Legal Bulletin No. 7A (June 7, 1999) included a number of sample comments concerning risk factors. These samples should be reviewed before drafting risk factors.

15. **When & How to Update Risk Factors:** There are many reasons why risk factors may need to be updated, and there are many methods of going about it. While different methods may make sense for different companies, it's important to understand the specific updating requirements.

    Item 1A of Part II of Form 10-Q requires companies to update their existing risk factor disclosure for "material changes." Updating may require incorporating changes to previously disclosed risks or disclosure of new risk factors based upon developments in the business. Only changes that are material will trigger an updating requirement—and there is no affirmative obligation to disclose that no reportable changes have occurred.

    Companies take different approaches to the updating requirement. Some include their entire risk factors section in each 10-Q, updating individual risks as necessary. Others opt to disclose only the new or modified risk factors. Modified risk factors may be disclosed in their entirety—or the company may opt to simply summarize the material change to the previously disclosed risk factors.

    We don't think that any one of these approaches is necessarily superior to any of the others, but in drafting updating disclosure, companies should bear in mind the "buried facts" doctrine. Under the "buried facts" doctrine, a disclosure is deemed inadequate if it is presented in a way that conceals or obscures the information sought to be disclosed. The doctrine applies when the fact in question is hidden in a voluminous document or is disclosed in a piecemeal fashion which prevents a reasonable shareholder from realizing the correlation and overall import of the various facts interspersed throughout the document. See, e.g., *Werner v. Werner*, 267 F.3d 288, 297 (3d. Cir. 2001).

    As a result, it may be appropriate to call out new disclosure in an appropriate fashion in a 10-Q filing if the company opts to republish its entire risk factors section in full. Once risk factors are updated in a 10-Q, they should continue to

be included in subsequent 10-Qs for the remainder of that fiscal year. The language of Form 10-Q provides the basis for this requirement. Form 10-Q expressly requires "any material changes from risk factors as previously disclosed in the registrant's Form 10-K" in response to Item 1A to Part 1 of Form 10-K.

Note that Form 8-K is also used to update risk factor disclosure. This most commonly occurs when companies are engaged in a shelf offering and want to make sure that the relevant information is incorporated by reference into the registration statement. Companies also sometimes opt to update risk factors through 8-K filings even without an ongoing shelf offering. Reasons for updating under these circumstances vary, but may include management's assessment that the materiality of the development in question makes it prudent to make an 8-K filing. Or it may reflect the fact that the development is attracting significant investor attention. In any event, new risk factors are typically included in an Item 8.01 Form 8-K, rather than under Item 7.01, because of the need to incorporate them into any effective Securities Act registration statements (including any Form S-8).

For more information, see our “Risk Factors Disclosure Handbook” - posted in our “Risk Factors” Practice Area on TheCorporateCounsel.net.

November 16, 2021

Audit Committee Disclosures: Audit Quality & Non-Financial Risks Getting More Attention

EY is out with their 10th annual survey of audit committee disclosures – finding that committees are continuing to share more info about their role and work. The survey primarily looks at 2021 proxy statements from Fortune 100 companies. It also includes stats about auditor ratification support and audit committee composition at a bigger group of companies. The areas with the most year-over-year change relate to audit quality & the committee's oversight role for non-financial risks. Here are some of the key takeaways:

> – This year, 71% of reviewed companies disclosed factors used in the audit committee's assessment of the external auditor qualifications and work quality, up from 64% last year. Only 15% of these companies made that disclosure in 2012.
>
> – Nearly 92% of reviewed companies disclosed that the audit committee considers non-audit fees and services when assessing auditor independence vs. just 16% in 2012.
>
> – Nearly 70% of reviewed companies stated that they consider the impact of changing auditors when assessing whether to retain the current external auditor, and 79% disclose the tenure of the current auditor. That's up from just 3% and 23%, respectively, in 2012.

EY also found that 76% of the reviewed companies included additional disclosures around risks beyond financial reporting that were being overseen by the audit committee. Some of these top risks being overseen by audit committees include cybersecurity, data privacy, enterprise risk management and ESG. Here's more detail on that piece:

> – Nearly 70% of reviewed companies disclosed that the audit committee oversees cybersecurity matters.
>
> – Notably, 10% of reviewed companies discussed the audit committee's role in ESG matters, up from 6% last year. These matters include oversight of climate change risks as they relate to financial and operational risk exposures and other environmental, health and safety-related matters.

On "Critical Audit Matters," EY found that 16 out of 72 companies discussed the audit committee's review and discussion of CAMs with the external auditors. Only one company noted the number of CAMs identified.

> As you prepare your disclosures for 2022, remember that our 49-page "Audit Committee Disclosure" Handbook can help you efficiently resolve questions that arise. It covers the regulatory requirements for audit committees as well as real-world disclosure trends.

– **Liz Dunshee**

Posted by Liz Dunshee

Permalink: https://www.thecorporatecounsel.net/blog/2021/11/audit-committee-disclosures-audit-quality-non-financial-risks-getting-more-attention.html

Checklist: Board Risk Oversight - Considerations

By TheCorporateCounsel.net

1. Increased Focus On Board Risk Oversight: Risk management has long been among the board's key oversight functions, but there has been intensified investor, regulator and company focus on this responsibility and how it is being effected – particularly in light of high-profile risk oversight failures and accompanying litigation.

The types, number, breadth and complexity of risks on the board's radar screen have been growing & evolving (for example, data & privacy security-related, regulatory and global operations-related risks - which were rarely among the chief concerns historically - are now front and center), and there is increased sensitivity to the critical nature of risk management - but the board's basic oversight responsibility has not changed. In 2009, in connection with its reversal of policy concerning the automatic excludability of risk evaluation-related shareholder proposals under Rule 14a-8(i)(7), the SEC noted that it had "become increasingly cognizant that the adequacy of risk management and oversight can have major consequences for a company and its shareholders."

The board's risk oversight responsibility includes:

- Overseeing and assessing the processes management uses to identify, evaluate, prioritize & manage risks
- Overseeing the company's major risks
- Together with management, agreeing on an appropriate company risk appetite/profile, i.e., the types & degree of risk the company is willing to accept in pursuit of its objectives (current and long-term)
- Ensuring the company's strategic plans are consistent with the agreed-upon risk profile
- Ensuring that compensation programs reward performance consistent with (and don't incentivize performance inconsistent with) the agreed-upon risk profile

Risk identification and management is also inherent in the company's strategic planning process - another of the board's critical oversight responsibilities, and should include an effective crisis management plan. See our separate checklists addressing the board's oversight of strategic planning – "Meeting Preparation," "Process" & "Agendas" – and our "Crisis Planning Checklist."

2. Top Focus: Annual benchmarking surveys – available in the "Corporate Governance Surveys" Practice Area on TheCorporateCounsel.net – consistently reflect that risk management is a valued skill for directors and that risk management is a top focus for boards, and is particularly challenging for complex global businesses. This is partly because the C-suite may have blind spots when it comes to emerging areas of risk. Key operational challenges include identifying risks – as well as analyzing & responding to risks.

3. Legal Requirements: SEC disclosure rules require proxy statement disclosure of the extent of the board's role in the risk oversight of the company - such as how the board administers its oversight function, and the effect that this has on the board's leadership structure. In addition, companies are required to discuss and analyze compensation policies and practices for all employees to the extent that the policies or practices create risks that are reasonably likely to have a material adverse effect on the company.

NYSE listing standards require the audit committee to have a written charter that addresses - among other things - the committee's responsibility to discuss policies with respect to risk assessment and risk management. The NYSE's commentary to this standard clarifies that

> "While it is the job of the CEO and senior management to assess and manage the company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the company's major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken."

Although the NYSE commentary sought to reassure companies that the audit committee's role vis a vis risk oversight is not expected to be all-encompassing, the standard has in fact continued to trigger a lot of confusion and angst about the audit

committee's responsibility in this area given its numerous other legally prescribed responsibilities. Nasdaq doesn't have a comparable requirement.

For many banks and other financial entities, Dodd-Frank also requires boards to maintain a risk committee that operates under a formal written charter. These committees operate under Federal Reserve oversight – even for smaller banks that establish them voluntarily. For non-financial companies, risk committees are not currently required by SEC or exchange listing rules.

4. Investor & Proxy Advisor Expectations: Major institutional investors and proxy advisors are not shy about expressing their expectations as to how the board should fulfill its risk oversight responsibilities, and this topic is increasingly receiving more attention in their policies. Here is just a sampling:

- **BlackRock:** Companies should have an established process for identifying, monitoring, and managing key risks. Independent directors should have ready access to relevant management information and outside advice, as appropriate, to ensure they can properly oversee risk management. We encourage companies to provide transparency around risk measurement, mitigation, and reporting to the board. We are particularly interested in understanding how risk oversight processes evolve in response to changes in corporate strategy and/or shifts in the business and related risk environment.

- **CII:** The board has ultimate responsibility for risk oversight. The board should (1) establish a company's risk management philosophy and risk appetite; (2) understand and ensure risk management practices for the company; (3) regularly review risks in relation to the risk appetite; and (4) evaluate how management responds to the most significant risks. In determining the risk profile, the board should consider the dynamics of the company, its industry and any systemic risks. Council policies on other critical corporate governance matters, such as executive compensation . . . reinforce the importance of the board's consideration of risk factors. Effective risk oversight requires regular, meaningful communication between the board and management, among board members and commit tees, and between the board and any outside advisers it consults, about the company's material risks and risk management processes. The board should disclose to shareowners, at least annually, sufficient information to enable them to assess whether the board is carrying out its oversight responsibilities effectively.

- **CalPERS:** The primary goal is to ensure companies adopt policies, operating procedures, reporting, and decision-making protocols to effectively manage, evaluate, and mitigate risk. The ultimate outcome is to ensure that companies function as "risk intelligent" organizations. CalPERS recommends the following:

  a. The board is ultimately responsible for a company's risk management philosophy, organizational risk framework and oversight. The board should be comprised of skilled directors with a balance of broad business experience and extensive industry expertise to understand and question the breadth of risks faced by the company. Risk management should be considered a priority and sufficient time should be devoted to oversight.

  b. The company should promote a risk-focused culture and a common risk management framework should be used across the entire organization. Frequent and meaningful communication should be considered the "cornerstone" for an effective risk framework. A robust risk framework will facilitate communication across business units, up the command chain and to the board.

  c. The board should set out specific risk tolerances and implement a dynamic process that continuously evaluates and prioritizes risks. An effective risk oversight process considers both internal company-related risks such as operational, financial, credit, liquidity, corporate governance, cyber-security, environmental, reputational, social, and external risks such as industry related, systemic, and macro-economic.

  d. Executive compensation practices should be evaluated to ensure alignment with the company's risk tolerances and that compensation structures do not encourage excessive risk taking.

  e. At least annually, the board should approve a documented risk management plan and disclose sufficient information to enable shareowners to assess whether the board is carrying out its risk oversight responsibilities. Disclosure should also include the role of external parties such as third-party consultants in the risk management process.

  f. While the board is ultimately responsible for risk oversight, executive management should be charged with designing, implementing and maintaining an effective risk program. Roles and reporting lines related to risk management should be clearly defined. At a minimum, the roles and

reporting lines should be explicitly set out for the board, board risk committees, chief executive officer, chief financial officer, the chief risk officer, and business unit heads. The board and risk related committees should have appropriate transparency and visibility into the organization's risk management practices to carry out their responsibilities.

- **TIAA-CREF:**

  - The Audit Committee oversees the company's accounting, compliance and in most cases risk management practices.

  - Each committee charter should specifically identify the role the committee plays in the overall risk management structure of the board. When a company faces numerous or acute risks, financially or operationally, the board should disclose why the current risk management structure is appropriate.

  - Compensation should include a mixture of cash and equity that is appropriate based on the company's compensation philosophy without incentivizing excessive risk.

- **ISS:** Under extraordinary circumstances, vote AGAINST or WITHHOLD from directors individually, committee members, or the entire board, due to [among other factors,] [m]aterial failures of governance, stewardship, risk oversight, or fiduciary responsibilities at the company. Examples of failure of risk oversight include, but are not limited to: bribery; large or serial fines or sanctions from regulatory bodies; significant adverse legal judgments or settlements; hedging of company stock; hedging of company stock; or significant pledging of company stock [by directors and/or executives]. In addition, risk oversight failures at the company are among the factors ISS will consider in assessing shareholder proposals calling for an independent board chair.

- **Glass Lewis:** Glass Lewis evaluates the risk management function of the board on a case-by-case basis. Sound risk management, while necessary at all companies, is particularly important at financial firms which inherently maintain significant exposure to financial risk. We believe such financial firms should have a chief risk officer reporting directly to the board and a dedicated risk committee or a committee of the board charged with risk oversight. Moreover, many non-financial firms maintain strategies which involve a high level of exposure to financial risk. Similarly, since many non-

financial firms have complex hedging or trading strategies, those firms should also have a chief risk officer and a risk committee.

When analyzing the risk management practices, we take note of any significant losses or write-downs on financial assets and/or structured transactions. In cases where a company has disclosed a sizable loss or write down, and where we find that the company's board-level risk committee's poor oversight contributed to the loss, we will recommend that shareholders vote against such committee members on that basis. In addition, in cases where a company maintains a significant level of financial risk exposure but fails to disclose any explicit form of board-level risk oversight (committee or otherwise), we will consider recommending to vote against the chairman of the board on that basis. However, we generally would not recommend voting against a combined chairman/CEO, except in egregious cases.

5. Allocation of Responsibilities: The increased scrutiny of the board's risk oversight responsibility has included an ongoing, healthy debate about the most effective board/committee risk oversight structure. As with most governance practices, there is no right or wrong approach. The important thing is that the board implement a structure that enables it to remain fully informed about - and understand - the company's major risks, and the processes the company uses to identify, monitor and manage those risks.

Annual benchmarking surveys – available in the "Corporate Governance Surveys" Practice Area on TheCorporateCounsel.net – show that the number of companies with standalone risk committees has increased in recent years. However, at the vast majority of companies, risk oversight continues to be a shared responsibility. A recent Society/Deloitte survey indicated that boards coordinate risk oversight by having committees share meeting minutes & materials and by having detailed discussions at the full board meeting.

See our separate "Checklist: Board Risk Oversight – Structure Types" – which addresses potential upsides and downsides associated with board risk committees and alternative risk oversight structures.

6. Board Composition Implications: The increased focus on the board's risk oversight responsibility in the context of recent crises has triggered a desire for increased representation on the board of directors with risk management experience. This is borne out in annual surveys that indicate that risk management expertise is one of the most desirable attributes for directors.

Having directors with industry expertise is also perceived to enhance the board's risk oversight effectiveness. Audit and risk committee chairs tend to say that directors with backgrounds in the company's industry are perceived as understanding the business such that they can fully appreciate the risk management challenges the company faces. Other attributes favorable to risk oversight effectiveness include financial expertise and diversity, i.e., outsider perspectives that could help boards think about risk in a new way.

See our separate “Board Matrices Checklist” and our "D&O Biographical/Director Qualifications & Skills Disclosure Handbook" posted on TheCorporateCounsel.net.

Checklist: Board Risk Oversight – Structure Types

By TheCorporateCounsel.net

1. Risk Oversight Structure Varies: Increased scrutiny of the board's risk oversight responsibility has triggered healthy debate about the most effective board/committee risk oversight structure. Boards commonly establish standing committees that are not required by law/listing standards and - even absent statutory requirements - often delegate significant responsibilities to their various standing committees in a manner uniquely suitable to their needs (which are associated with company size, industry, complexity, etc.), size, composition and structure.

Along those lines, there are various potential approaches to effecting risk oversight - and there is no right or wrong approach. The important thing is that the board acknowledge its responsibility to provide effective risk oversight - and implement a structure and allocate responsibilities in a way that enables it to fulfill this responsibility effectively.

See our separate checklists addressing board standing committee structure and how boards commonly allocate risk oversight responsibilities and other risk oversight considerations – posted in the "Board Committees" Practice Area on TheCorporateCounsel.net.

2. Pros & Cons of Different Approaches: Although committee structure, functions and responsibilities should always be tailored to your company's facts and circumstances (except when precluded by law), it's helpful to be aware of some of the commonly debated factors associated with particular structures that may influence your consideration of the most optimal approach for your company.

The risk oversight structure debate usually centers around whether the board should establish a separate risk committee, delegate primary oversight responsibility to the audit committee, or retain primary responsibility at the board level (even assuming delegation to committees of specific types of risks inherent in or consistent with their areas of responsibility).

Annual benchmarking surveys – available in the "Corporate Governance Surveys" Practice Area of TheCorporateCounsel.net – show that companies are increasingly establishing standalone risk committees (or risk & finance committees) – but it's still not a majority practice. The most common approach is to assign risk oversight to the audit committee, followed by the full board, and to assign oversight of committee-specific risks (e.g. risks from compensation programs) on an ad-hoc

basis. However, surveys show that most directors believe that the full board should oversee risk, rather than the audit committee. Allocating this responsibility to the audit committee has declined considerably over the last decade.

Consider these factors in connection with the most common alternative structures:

– **Dedicated Risk Committee:**

Factors weighing in favor:

- Can be more effective at oversight of numerous, complex, inter-related risks than audit and other board-level committees whose responsibilities are more narrowly focused
- Focuses director attention on most critical risks and risk management capabilities
- Keeps issue on management's and board's agenda
- Keeps current on risks and related factors (e.g., regulatory issues) in a way that can be difficult for other committees to achieve
- Ensures company stays focused on the right risk management priorities
- Facilitates sharper focus on risks, risk management and full range of risks company faces through additional time devoted without other topics crowding agenda
- Provides continuous view of risk - which is helpful in context of dynamic nature of risk
- May be a better fit for companies with rapidly changing business environments and expecting significant emerging risks
- Fosters integrated, enterprise-wide approach to identifying and managing risk
- Provides an impetus toward improving the quality of risk reporting and monitoring - both for management and the board - which can assist the board in focusing on the "big picture"

- Provides greater support for executives with broad risk management responsibilities - resulting in a stronger focus at the board level on the adequacy of resources allocated to risk management.

- Allows audit committee and other board committees to focus on their respective core responsibilities

Factors weighing against:

- Directors may be reluctant to add another committee given the time commitment required and the likelihood that they are already serving on multiple committees

- Would need to coordinate and regularly communicate with audit and other committees to accommodate and benefit from their risk oversight activities

- Absent independent directors with deep knowledge and experience in dealing with the industry and its critical risks, separate risk committee won't be effective

- Can't overcome gaps in company's risk management process even if properly composed and optimally structured

- Effectiveness is highly dependent on information and insights from management and external sources

- Potential for duplication of efforts arising from risk oversight activities of other board committees

- Adding additional board committee can dilute board's focus in context of other committee work

- Adding additional board committee increases scheduling and other administrative challenges

- Tendency for other directors to shy away from risk matters because of delegation to separate risk committee

– **Audit Committee:**

Factors weighing in favor:

- Already charged by NYSE listing standards with discussing guidelines and policies to govern the process by which risk assessment and management is undertaken

- Already has oversight responsibility for financial reporting and internal control-related risks - which inherently encompass numerous other types of risks

- If risk profile changes infrequently and is narrowly focused, audit committee may capably assume risk oversight as natural adjunct to other responsibilities

- Given that audit committee is required to maintain some risk oversight responsibility, full delegation avoids potential that issues delegated to multiple committees could fall between the cracks

- Some directors who favor a powerful, global audit committee oppose formation of a separate risk committee because it can dilute the audit committee's power

Factors weighing against:

- Audit committee may lack the time, skills and support to assume primary responsibility given its numerous other responsibilities

- Risk oversight is time consuming and, in view of audit committee's other responsibilities, could translate to day-long meetings for the committee

- Financial expertise/acumen represented on audit committee may be insufficient to evaluate policies for assessing and managing the wide range of business and operational risks the company faces

- Number, types and complexity of company's risks may be inconsistent with delegation of primary responsibility to already overburdened audit committee

- In that so much of the audit committee's traditional agenda is time and date-sensitive, risk oversight may inevitably and consistently become lower priority simply due to insufficient time and resources

- **Full Board:**

Factors weighing in favor:

- Always retains overall responsibility for risk oversight in any event
- Doesn't preclude delegation of oversight of certain risks to specific board committees - which is often the case
- Needs to fully understand major risks, and how risks are monitored and managed, in order to effectively fulfill strategic planning and other oversight responsibilities
- Doesn't preclude delineation of board's main areas of focus (e.g., strategic, financial and execution risks associated with the business and strategic plans) relative to focus of standing committees (see Honeywell's "Board's Role in Risk Oversight" disclosure in its 2018 proxy statement for an excellent example of this approach)

Factors weighing against:

- Lacks benefits of independent director oversight associated with key standing committees
- Most of the factors that weigh in favor of a dedicated risk committee arguably weigh against the full board retaining primary oversight responsibility

3. Shared Committee Oversight: In recognition of the fact that many types of risks are already inherent in the scope of responsibilities assigned to their existing committees, a number of companies allocate risk oversight responsibilities across multiple or all of the board's standing committees. In this event, effectively coordinating the activities of the committees is critical to an effective oversight process.

The most common practices implemented to ensure coordination are:

- Holding detailed discussions at full board meetings
- Sharing minutes or other meeting materials
- Cross membership of committees

- Holding joint meetings
- Risk presentations repeated at multiple committee meetings
- Some combination of these practices

See our separate checklist addressing allocation of responsibilities to the board's standing committees – posted in the "Board Committees" Practice Area on TheCorporateCounsel.net – and the numerous other resources posted in our "Risk Management" Practice Area on TheCorporateCounsel.net.

February 16, 2023

Risk & Crisis Management: Directors Need to "Roll Up Their Sleeves"

High-profile *Caremark* cases and SEC enforcement actions have focused attention on the ever-higher expectations placed on boards when it comes to risk oversight. This article from Nasdaq's Center for Board Excellence says that when it comes to risk oversight and crisis management, stakeholders expect directors to roll up their sleeves:

> Given the rapidity at which information and news travel today, boards need to be prepared to act when setbacks happen, and crisis management cannot be delegated to executive teams. Shareholders expect the board to actively help navigate all phases of a crisis, from the initial "hair-on-fire" through the post-mortem. One of the most important things for boards to do is to engage, as shareholders and stakeholders expect the board to ensure that appropriate processes are in place to successfully manage a crisis.
>
> The board's role is to ensure the company has the right processes and people in place to effectively identify and evaluate risk, in addition to approving the risk appetite of the firm on behalf of stakeholders. Developing the risk appetite is critical as it frames how the board will react to any risk-related setback. Boards may consider collaborating with management to establish a risk appetite statement, approaching risk from a macro level. While identifying every single risk is unrealistic, this practice promotes discipline in setting a foundation for enterprise risk

The article says that boards need to understand how information flows through their organization in order to better anticipate unforeseen events. That review should incorporate an assessment of whether information from all viewpoints is welcome, or if the company's culture is to disregard points of view that may potentially conflict with the general consensus of top management.

– **John Jenkins**

Posted by John Jenkins
Permalink: https://www.thecorporatecounsel.net/blog/2023/02/risk-crisis-management-directors-need-to-roll-up-their-sleeves.html

September 13, 2021

Risk Oversight In the Era of "Easier" Caremark Claims

Last week, Vice Chancellor Zurn of the Delaware Court of Chancery determined that the shareholder derivative litigation against Boeing's board of directors could proceed, based on allegations that the directors breached their duty of loyalty by not making a good faith effort to implement an oversight system and monitor it. The court dismissed the shareholders' claims against the officers and the board for compensation decisions.

In light of the tragic loss of life that formed the basis for this lawsuit, the allegations here about the shortcomings in director decision-making are troubling, and that may have affected the opinion. The court noted that:

> – Meeting minutes didn't indicate rigorous director discussions of safety issues
>
> – No board committee was charged with direct responsibility to monitor safety
>
> – The board didn't direct management to provide regular safety updates – it "passively" received updates at management's discretion
>
> – The Board publicly lied about whether & how it monitored the 737 MAX's safety in order to preserve its reputation

Based on this, VC Zurn held that the board came up short on both *Caremark* prongs: it failed to establish a monitoring system and failed to respond to red flags. She also found that the plaintiffs adequately alleged scienter. Alarmingly for companies and their advisors, VC Zurn determined that the board's remedial step of creating a safety committee after the crashes was evidence that, before the crashes, it had no oversight process at all – and knew it.

For 25 years, it was notoriously difficult for a *Caremark* claim to survive a motion to dismiss, even though the court has to accept the plaintiffs' allegations as true at that stage of litigation. VC Zurn even acknowledged in her opinion that it's extremely difficult to plead an oversight failure. Yet, a series of *Caremark* claims have proceeded past the motion to dismiss stage in just the past couple of years. As this Wachtell Lipton memo notes, that's a big deal for the company and the board:

> The company's directors now face the prospect of intrusive document discovery, extensive depositions, and either an expensive settlement or a trial to defend the effectiveness of their oversight.

UCLA's Stephen Bainbridge blogged that this case is another sign that *Caremark* claims are getting easier. He notes that the court took a much closer – and less favorable – look at board decisions than what you'd expect. Yet, as Kevin LaCroix blogged, the crashes at issue here "dramatically highlighted the critical importance of safety issues for Boeing." And – hopefully – these types of events are rare. So, it's too early to declare that every duty-of-oversight claim will proceed to the merits. But Kevin notes:

> All of that said, I do think the recent spate of breach of the duty of oversight cases will encourage plaintiffs to pursue these kinds of claims and to include claims of breach of the duty of oversight in cases in which companies have experienced significant adverse circumstances in important operations. I suspect we are going to see an increase of claims of this type.

That makes it all the more important for other boards to review their risk management processes right now. Helpful steps could be:

> – Document the board's oversight of enterprise risk management, its process for asking questions & reviewing risks, and its evaluation of which functions are "mission critical"
>
> – Ensure the board has a robust oversight process for key functions that create significant risk – and consider forming a dedicated board committee
>
> – Document regular risk reporting to the committee & board, directors' rigorous discussions & questions about risks, and board-directed risk reports

– **Liz Dunshee**

Posted by Liz Dunshee
Permalink: https://www.thecorporatecounsel.net/blog/2021/09/risk-oversight-in-the-era-of-easier-caremark-claims.html

Comment Letter Trend: SEC Seeks Expanded Discussion of Board's Role in Risk Oversight

February.13.2023

During 2022 the SEC issued at least 36 comment letters requesting expanded discussion about the board's role in risk oversight. We summarize below the basic requirements of this disclosure and the most common new elements requested by the SEC through its comment letters issued during 2022. We encourage all issuers to consider these elements as they prepare for the 2023 proxy season.

As required by Item 407(h) of Regulation S-K, proxy statements addressing the election of directors must contain a discussion about "*the extent of the board's role in the risk oversight of the [company], such as how the board administers its oversight function, and the effect that this has on the board's leadership structure*." In the 2009 adopting release for Item 407(h), the SEC provided the following additional guidance:

> "*This disclosure requirement gives companies the flexibility to describe how the board administers its risk oversight function, such as through the whole board, or through a separate risk committee or the audit committee, for example. Where relevant, companies may want to address whether the individuals who supervise the day-to-day risk management responsibilities report directly to the board as a whole or to a board committee or how the board or committee otherwise receives information from such individuals*."

Our review of the comment letters issued during 2022 requesting expanded Item 407(h) disclosures suggests the SEC now also expects a discussion of the following common elements:

1. Whether and why a company's board would choose to retain direct oversight responsibility for certain material risks (particularly cybersecurity, ESG and sustainability related risks) rather than assign oversight to a board committee;
2. The timeframe over which a company evaluates risks (e.g., short-term, intermediate-term, or long-term) and how a company applies different oversight standards based upon the immediacy of the risk assessed;
3. Whether a company consults with outside advisors and experts to anticipate future threats and trends, and how often it reassesses its risk environment;
4. How a company's board interacts with management to address existing risks and identify significant emerging risks;
5. Whether a company has a Chief Compliance Officer, or person serving in a similar role, and to whom this position reports; and
6. How a company's risk oversight process aligns with its disclosure controls and procedures.

Given the frequency of these comments over the past year, issuers should consider addressing the above elements in their discussion of the board's role in risk oversight. Companies with material cybersecurity risk or with publicly made statements about climate risks should take particular care to address the first element listed above with respect to those types of risks in their discussion of the board's role in risk oversight.

Authors

J. T. Ho
Partner, Corporate Governance, Capital Markets

San Francisco Office

D +1 415 773 5624
E jho@orrick.com

Hong Tran
Associate, Corporate Governance, Environmental, Social & Corporate Governance (ESG)

Houston

D +1 713 658 6452
E htran@orrick.com

Bobby Bee
Practice Support Counsel, Capital Markets

New York Office

D +1 212 506 5000
E rbee@orrick.com

Checklist: Proxy Disclosure - Board Oversight of Risk

By Howard Dicker, Weil, Gotshal & Manges[1]

Proxy statements reveal that boards execute their risk oversight responsibilities according to a number of considerations and processes:

1. Risk Oversight Versus Risk Management

- **Approach Resources, Inc.** – "Assessing and managing risk is the responsibility of the management of the Company. However, the Board has an active role, as a whole, and also at the committee level, in overseeing management of the Company's risks. The Board regularly reviews information regarding the Company's credit, liquidity and operations, as well as the risks associated with each, and discusses the same with management."

- **ConocoPhillips** – "While our management team is responsible for the day-to-day management of risk, the Board has broad oversight responsibility for our risk-management programs. In this role, the Board is responsible for satisfying itself that the risk-management processes designed and implemented by management are functioning as intended, and that necessary steps are taken to foster a culture of prudent decision-making throughout the organization…"

- **Procter & Gamble** – "The Company's senior management has the responsibility to develop and implement the Company's strategic plans, and to identify, evaluate, manage, and mitigate the risks inherent in those plans. It is the responsibility of the Board to understand and oversee the Company's strategic plans, the associated risks, and the steps that senior management is taking to manage and mitigate those risks. The Board takes an active approach to its role in overseeing the development and execution of the Company's business strategies as well as its risk oversight role. This approach is bolstered by the Board's leadership and committee structure, which ensures proper consideration and evaluation of potential enterprise risks by the full Board under the auspices of the Chairman of the Board and Lead Director, and further consideration and evaluation of certain risks at the committee level.

[1] With appreciated assistance from Audrey Susanin.

As part of its strategic risk management oversight, the full Board conducts a number of reviews throughout the year to ensure that the Company's strategy and risk management is appropriate and prudent, including: [lists activities]

In addition, the Board has delegated certain risk management oversight responsibilities to specific Board committees, each of which reports regularly to the full Board…"

2. Coordination of Management and the Board to Address Risk

- **Boeing** – "Senior management is responsible for day-to-day management of risk, including the creation of appropriate risk management policies and procedures. The Board is responsible for overseeing management in the execution of its risk management responsibilities and for assessing the Company's approach to risk management. The Board regularly assesses significant risks to the Company in the course of reviews of corporate strategy and the development of our long-range business plan, including significant new development programs. As part of its responsibilities, the Board and its standing committees also regularly review strategic, operational, financial, compensation, and compliance risks with senior management. Examples of risk oversight activities conducted by the Board's Committees, subject to Committee report-outs and full discussion at the Board level, are set forth below."

- **Oneok, Inc.** – "The Board implements its risk oversight responsibilities by having management provide periodic briefing and informational sessions on the significant voluntary and involuntary risks that the company faces and how the company is seeking to control and mitigate risk if and when appropriate. In some cases, as with risks relating to significant acquisitions, risk oversight is addressed as part of the full Board's engagement with the Chief Executive Officer and management.

  The Board annually reviews a management assessment of the various operational and regulatory risks facing our company, their relative magnitude and management's plan for mitigating these risks. This review is conducted in conjunction with the Board's review of our company's business strategy at its annual strategic planning meeting and at other meetings as appropriate.

We also maintain a Risk Oversight and Strategy Committee, which consists of members of our senior management…"

- **Pfizer** – "Management is responsible for assessing and managing risk, including through the Enterprise Risk Management (ERM) program, subject to oversight by the Board. The ERM program provides a framework for risk identification and management. Each risk is assigned to a member or members, as appropriate, of our Executive Leadership Team (ELT) — the heads of our principal businesses and corporate functions. The Board believes that its leadership structure and the ERM program support the risk oversight function of the Board.

  … The Board considers specific risk topics, including, among others, risks associated with our strategic plan, our capital structure, and our R&D activities. In addition, the Board receives regular reports from members of our ELT that include discussions of the risks involved in their respective areas of responsibility. The Board is routinely informed of developments that could affect our risk profile or other aspects of our business…"

3. <u>Risk Oversight and Leadership Structure</u>

- **IBM** – "The Board's role in risk oversight of the Company is consistent with the Company's leadership structure, with the CEO and other members of senior management having responsibility for assessing and managing the Company's risk exposure, and the Board and its committees providing oversight in connection with those efforts."

4. <u>Alignment of Risk with Corporate Strategy</u>

- **Advanced Micro Devices, Inc.** – "…At least annually, the Board discusses with management the appropriate level of risk relative to our strategy and objectives and reviews with management our existing risk management processes and their effectiveness…"

- **Anthem, Inc.** – "Our Board of Directors oversees the risk management processes that have been designed and are implemented by our executives to determine whether those processes are functioning as intended and are consistent with our business and strategy."

- **Destination XL Group, Inc.** – "The involvement of the full Board of Directors in setting our business strategy is a key part of its oversight of risk

management and in determining what constitutes an appropriate level of risk for us."

5. Board's Role in Setting the Company's "Risk Appetite"

- **Bank of America** – "Risk is inherent in all of our business activities. One of the tenets of Responsible Growth is "we must grow within our risk framework." We execute on that strategy through our commitment to responsible and rigorous risk management and through a comprehensive approach with a defined Risk Framework and a well-articulated Risk Appetite Statement. The Risk Framework and Risk Appetite Statement are regularly reviewed with an eye towards enhancements and improvements. The Risk Framework sets forth clear roles, responsibilities, and accountability for the management of risk and describes how our Board oversees the establishment of our risk appetite and of both quantitative limits and qualitative statements and objectives for our activities. This framework of objective, independent Board oversight and management's robust risk management better enables us to serve our customers, deliver long-term value for our stockholders, and achieve our strategic objectives…"

- **Innophos Holdings, Inc.** – "The Board is ultimately responsible for approving the Company Enterprise Risk Management framework and key risk management policies, including risk appetite parameters. It approves the overall Company strategy to ensure it fits with risk appetite …"

- **JPMorgan Chase & Co.** – "The Directors' Risk Policy Committee [a]ssists the Board in its oversight of the Firm's global risk management framework, approves the primary risk management policies of the Firm and oversees management's responsibilities to assess and manage… [t]he governance frameworks or policies for risk identification, risk appetite, operational risk, reputation risk, compliance risk including fiduciary risk, and conduct risk…

  The Firm has an Independent Risk Management ("IRM") function, which consists of the Risk Management and Compliance organizations. The CEO appoints, subject to DRPC approval, the Firm's Chief Risk Officer to lead the IRM organization and manage the risk governance framework of the Firm. The risk governance framework is subject to approval by the DRPC in the form of the primary risk management policies.

  Certain risks, such as strategic risk, are overseen by the full Board. Board committees support the Board's oversight responsibility by overseeing the

risk categories related to such committee's specific area of focus. Each committee oversees reputation and conduct risk issues within its scope of responsibility. Risk issues that overlap committee responsibilities are reported to each committee overseeing such risk; when appropriate, relevant Board committees hold joint meetings…"

6. Role of the Audit Committee in Risk Oversight

- **3M** – "The Board has delegated to the Audit Committee through its charter the primary responsibility for the oversight of risks facing the Company. The charter provides that the Audit Committee shall 'discuss policies and procedures with respect to risk assessment and risk management, the Company's major risk exposures and the steps management has taken to monitor and mitigate such exposures.' … The Auditor periodically reviews with the Audit Committee the major risks facing the Company and the steps management has taken to monitor and mitigate those risks. …"

- **Alcoa** – "The Audit Committee discusses the Company's risk profile, risk management, and exposure (and Alcoa's policies relating to the same) with management, the internal auditors, and the independent auditors. Such discussions include the Company's major financial risk exposures and the steps management has taken to monitor and control these exposures. The Audit Committee also is charged with oversight of Alcoa's risks relating to cybersecurity, including review of the state of the Company's cybersecurity, emerging cybersecurity developments and threats, and the Company's strategy to mitigate cybersecurity risks."

- **Approach Resources, Inc.** – "Under its charter, the Audit Committee reviews and discusses with management the Company's major financial and other risk exposures and the steps management has taken to monitor and control such exposures, including the Company's risk assessment and risk management policies. In addition, the Audit Committee oversees risks related to the Company's financial statements, the financial reporting process, accounting, tax and legal matters, as well as liquidity risks and guidelines, policies and procedures for monitoring and mitigating risks.

  The Audit Committee meets regularly in executive session without the Company's independent public accounting firm and without management. Members of the Audit Committee routinely observe meetings of the Company's Disclosure Committee, which meets before the Company files quarterly and annual financial reports with the SEC. In addition, the Audit

Committee reviews and discusses with management and the Company's independent public accounting firm any major issues as to the adequacy of the Company's internal controls, any special steps adopted in light of material control deficiencies and the adequacy of disclosures about changes in internal control over financial reporting. The Audit Committee also meets with our internal controls, Sarbanes-Oxley compliance and enterprise risk management consultants, and, if applicable, reviews related-party transactions for potential conflicts of interest. Finally, the Audit Committee oversees the reserves estimation process and meets with our CEO, key management and our independent engineering firm to review the processes used to prepare our proved reserves reports."

- **Skyline Corp.** – "…The Audit Committee considers audit, accounting and compliance risk, and it receives reports from its outside auditors, internal audit staff, and the Chief Financial Officer, among others. The Audit Committee is also responsible for the review of Skyline's major risk exposures (whether financial, operational or otherwise), and the steps management has taken to monitor and control such exposures, and for evaluating management's process to assess and manage Skyline's enterprise risk issues…"

7. Role of Other Committees in Risk Oversight

- **3M** – "While the Board's primary oversight of risk is with the Audit Committee, the Board has delegated to other committees the oversight of risks within their areas of responsibility and expertise. For example, the Compensation Committee oversees the risks associated with the Company's compensation practices, including an annual review of the Company's risk assessment of its compensation policies and practices for its employees. The Finance Committee oversees risks associated with the Company's capital structure, its credit ratings and its cost of capital, long-term benefit obligations, and the Company's use of or investment in financial products, including derivatives used to manage risk related to foreign currencies, commodities, and interest rates. The Nominating and Governance Committee oversees the risks associated with the Company's overall governance and its succession planning process to understand that the Company has a slate of future, qualified candidates for key management positions."

- **Alcoa** – "…In addition [to the Audit Committee], the Safety, Sustainability and Public Issues Committee considers risks related to the Company's

reputation, and risks relating to safety and health, public policy, environmental sustainability, and social issues. The Governance and Nominating Committee considers risks related to corporate governance, and oversees succession planning for the Board and the appropriate assignment of directors to the Board committees for risk oversight and other areas of responsibilities. The Compensation and Benefits Committee considers risks related to the attraction and retention of talent, the design of compensation programs and incentive arrangements, and the investment management of the Company's principal retirement and savings plans. The Compensation and Benefits Committee periodically reviews Alcoa's incentive structure to avoid encouraging material risk taking through financial incentives. Based on these determinations, the Company believes that it is not reasonably likely that Alcoa's compensation and benefit plans incentivize undue risk or create risks that are reasonably likely to have a material adverse effect on us. See '*Compensation Discussion and Analysis—Executive Compensation Policies and Practices—What We Do—Maintain a Conservative Compensation Risk Profile*.'"

- **Approach Resources, Inc.** – "The Compensation Committee oversees the management of risks associated with executive compensation, and meets regularly in executive session without management. See "Compensation Practices as They Relate to Risk Management" for additional discussion of the Compensation Committee's oversight of risks relating to executive compensation. The Nominating and Governance Committee oversees the management of risks associated with corporate governance practices and procedures, including independence of the Board, and makes recommendations to the Board regarding improvements. While each committee is responsible for overseeing the management of certain risks, the entire Board is regularly informed through committee reports about such risks."

- **Skyline Corp.** – "…The Compensation Committee considers the level of risk implied by Skyline's compensation programs, including incentive compensation programs in which the CEO and other employees participate. The Nominating and Governance Committee monitors potential risks to the effectiveness of the Board, notably Director succession and the composition of the Board, and the principal policies that guide Skyline's governance…"

8. <u>Risk Management Experience as a Director Qualification</u>

- **Bank of America** – "Our directors bring relevant risk management oversight experience; see 'Our Director Nominees' on page 5."

- **Coca Cola** includes a table that summarizes certain key characteristics of the Company's business and the associated qualifications, attributes, skills and experiences that the Board believes should be represented on the Board. In light of the fact that "[t]he Board's responsibilities include understanding and overseeing the various risks facing the Company and ensuring that appropriate policies and procedures are in place to effectively manage risk," the Board believes that "Risk oversight/management expertise" is a qualification that should be represented on the Board.

- **Procter & Gamble** lists the following in its list of experiences, skills and qualifications that its directors bring to the board: "Leadership, strategy, and risk management experience. Directors with significant leadership experience over an extended period, including former chief executive officers, provide the Company with special insights. These individuals demonstrate a practical understanding of how large organizations operate, including the importance of talent management and how employee and executive compensation are set. They understand strategy, productivity, and risk management, and how these factors impact the Company's operations and controls. They possess recognized leadership qualities and are able to identify and develop leadership qualities in others."

- **UnitedHealth Group** lists "[r]isk oversight ability with respect to the particular skills of the individual director" as a "core criteria that every member of the Board should meet."

ESG-Related Risk Factors

2 minute read
February.15.2023

Companies should make sure they are considering emerging practices for disclosing environmental-, social-, and governance- ("ESG") related risk factors, as these disclosures are now a common practice.

- Based on our review of companies in the S&P 500, the number of companies with an ESG-related risk factor has increased year-over-year, in the period from 2019 to 2022. Risk factors spanned a range of ESG-related topics, primarily related to climate change, but also including diversity-, other environmental-, or general ESG-related risks. We expect this trend to be followed by small- and mid-cap companies. To see the graph that shows the percentage of the S&P 500 with an ESG-Related Risk Factor in the annual report (by fiscal year), please see this guest post for TheCorporateCounsel.net: ESG-Related Risk Factors: Nearly All S&P 500 Co's Now Have Them →.
- Climate-related risks accounted for most ESG-related risk factors in the S&P 500, with a significant increase in the number of companies reporting climate related risks since 2019.
- Most climate-related risk factors were specific to the reporting company's business. The most common type of climate-related risks reported for fiscal year 2021 were physical risks related to business operations, including potential disruptions in the supply chain due to climate related events and the direct exposure of company assets and operations to more severe hurricanes and wildfires.
- In the upcoming years, we expect more disclosures with respect to climate-related legal and regulatory risks, given the SEC's proposed climate-related disclosure rules, which are expected to be finalized this year, and the European Union's Corporate Sustainability Reporting Directive, which went into effect this year.
- To see the percentage breakdown of the S&P 500 (by industry) with a specific Climate-Related Risk Factor in the annual report (by fiscal year), please see this guest post for TheCorporateCounsel.net: Categories of Climate-Related Risk Factors: Data By Industry →.
- In addition to the growing number of ESG-related risk factors, we've seen an increase in the number of ESG-related risks specific to the reporting company's business, rather than "general" or "other" risks. To see examples of specific vs general ESG risk factor and the percent of S&P 500 companies that has specific ESG-related risk factors, please see this guest post for TheCorporateCounsel.net: ESG-Related Risk Factors: Getting More Specific →.
- Not every company will have ESG- or climate-related risk factors. But regardless of your industry, if you do not have a process in place to identify material company-specific ESG-related risks, especially climate-related risks, there is a potential that your risk management processes and disclosures will fall behind market practices.

Authors

J. T. Ho
Partner, Corporate Governance, Capital Markets

San Francisco Office

D +1 415 773 5624
E jho@orrick.com

Carolyn Frantz
Senior Counsel

Seattle

D +1 206 839 4402
M +1 773 704 6201
E cfrantz@orrick.com

Bobby Bee
Practice Support Counsel, Capital Markets

New York Office

D +1 212 506 5000
E rbee@orrick.com

Hayden Goudy
Director of Environmental, Social and Governance and Corporate Governance

Seattle

D +1 206 839 4356
E hgoudy@orrick.com