Deloitte.

Center for Board Effectiveness

On the audit committee's agenda

Who's in charge: The audit committee's role in ethics and compliance oversight

Background

Corporate compliance and ethical behavior (or their absence) are not new topics; corporate scandals and misdeeds have generated media and public interest for decades. However, beginning in the 1990s, a series of court decisions reminded boards and managements alike that their duties include oversight of these areas and that they can be held responsible when the lack of oversight results in ethical and compliance lapses.

The first such reminder of board oversight responsibility for compliance occurred in the Caremark case decided by the Delaware Chancery Court in 1996. In that case, the Court stated that this responsibility stems from the directors' duty to act in good faith and to be "reasonably informed concerning the corporation" and "that the corporation's information and reporting system [must] in concept and design [be] adequate to assure the board that appropriate information will come to its attention in a timely manner as matter of ordinary operations."[1]

The many court decisions that have subsequently reinforced board oversight responsibility for ethics and compliance have involved cases relating to lapses occurring in a variety of contexts: contaminated ice cream, product defects, and sexual harassment in the workplace, among other matters. In cases of this type, the Delaware courts have stated that corporate boards need to make good-faith efforts to exercise the fiduciary duty of care and that a failure to make those efforts breaches the fiduciary duty of loyalty.

Of course, courts were and are not the only ones calling for board oversight and accountability. As noted above, ethical and compliance breakdowns have long generated media and public interest in the role of the board. Consequently, regardless of whether a financial scandal, an industrial accident, mere negligence, or some other omission is involved, the question "Where was the board?" is not uncommon.

[1] In Re Caremark International, Inc., Delaware Court of Chancery, 698 A.2d 959.

감사위원회의 윤리 및 컴플라이언스 감독 역할

배경

기업 컴플라이언스와 윤리적 행동(또는 윤리적 행동의 부재)은 새로운 주제가 아닙니다. 수십 년 동안 기업 스캔들과 부정행위는 언론과 대중의 관심을 끌었습니다. 그러나 1990년대부터 법원 판결들은 이러한 영역을 감독하는 것이 이사회와 경영진의 의무에 포함되며, 감독 부족으로 인한 윤리 및 컴플라이언스 문제가 발생할 경우 그들이 책임을 질 수 있다는 것을 상기시켜 주었습니다.

1996년 델라웨어주 형평법법원에서 판결된 Caremark 사건은 기업 컴플라이언스에 대한 이사회의 감독 책임을 최초로 상기시킨 사건이었습니다. 이 사건에서 법원은 해당 책임이 이사들이 선의로 행동하고 "회사에 대해 합리적으로 정보를 알고" 있어야 하는 이사회의 의무에서 비롯된다고 하였습니다. 또한 법원은 "회사의 정보 및 보고 시스템이 개념적으로도 설계적으로도 충분하여 일상적인 운영의 일환으로 적절한 정보가 이사회의 주의를 적시에 끌 수 있도록 보장되어야 한다"고 명시했습니다.[1]

윤리 및 컴플라이언스에 대한 이사회 감독 책임을 강화하는 여러 법원 판결들은 다양한 맥락에서 발생한 결함에 관련된 사례들을 다루고 있습니다. 오염된 아이스크림, 제품 결함, 직장 내 성희롱 등의 문제가 포함됩니다. 이러한 사례에서 델라웨어 법원은 기업 이사회가 선관주의 의무와 감시의무를 이행하기 위해 노력해야 하며, 이러한 노력을 하지 않는 경우 충실의무를 위반하는 것으로 간주된다고 밝혔습니다.

물론 법원만이 이사회의 감독과 책임을 요구하는 것은 아닙니다. 앞서 언급한대로 윤리 및 컴플라이언스 결함은 오랜 기간 동안 언론과 대중의 이슈를 불러일으키며, 이사회의 역할에 대한 관심을 높였습니다. 그 결과 금융 스캔들, 산업 재해, 단순 과실 또는 기타 누락사항과 관련된 경우에도 "문제가 발생되는 동안 이사회는 무엇을 했는가?"라는 이사회 역할에 대한 질문은 드물지 않게 제기됩니다.

The audit committee's role

The cases referred to earlier and similar rulings make it clear that the board's oversight duties extend to compliance and ethics. However, those cases have not focused on where in the board structure these duties should reside.

To some extent, that governance gap has been addressed by statute and regulation. The Sarbanes-Oxley Act of 2002, enacted to a large degree in response to a series of financial reporting scandals in the late 1990s and early 2000s, made it clear that at least some of these duties belong to the audit committee. Specifically, Securities and Exchange Commission (SEC) Rule 10A-3, implementing a provision of Sarbanes-Oxley, states that "[e]ach audit committee must establish procedures for the receipt, retention, and treatment of complaints … regarding accounting, internal accounting controls, or auditing matters … and [t]he confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters." As a result of this rule, public companies that did not already have employee hotlines were well advised to install them and to report certain complaints and concerns to the audit committee.

While hotlines may have been implemented initially to deal with accounting and auditing matters, they have inevitably become repositories for a wide variety of employee concerns, ranging from code of conduct violations to hostile work environment matters to general complaints and suggestions. However, rather than develop a separate process for reporting non-audit and accounting matters to others within the company, at many companies the audit committee received—and continues to receive—reports on many of such matters. Consequently, the audit committee often exercises the ultimate governance oversight function for many types of employee complaints and concerns.

The audit committee's responsibilities and resources

While it may have ultimate oversight of such matters, the audit committee has extensive responsibilities other than those associated with compliance and ethics. Accordingly, it is appropriate for the committee to consider whether it is the proper committee to oversee a particular area of compliance. For example, there are certain types of risks—generally not involving financial and accounting matters—that may more properly be overseen by the compensation or nominating/governance committee, thereby conserving the audit committee's resources for matters that more directly relate to its key areas of risk management oversight.

The committee can also consider the processes by which it receives and reviews information relating to compliance and ethics. For example, at many companies, the audit committee is the only board-level committee that receives reports of hotline submissions. Given the number of submissions and the fact that many submissions typically do not involve areas relevant to the audit committee's jurisdiction, the committee may opt to review only select submissions that meet a defined threshold of severity or subject matter relevance, delegating to management liaisons responsibility to assure that no legitimate submissions slip through the cracks and/or to report to the committee on trends or on issues raised in submissions directed to other committees or members of management. Logistical concerns may also increase as companies expand the use of hotlines to other stakeholder

On the audit committee's agenda | US

감사위원회의 역할

앞서 언급한 사례들과 유사한 판결들은 이사회의 감독 의무가 컴플라이언스 및 윤리에도 적용되어야 함을 명백하게 보여줍니다. 그러나 이러한 사례들은 이사회의 감독 의무가 이사회 구조 내 어떤 위치에 속해야 하는지에 대해서는 집중적으로 다루지 않았습니다.

이러한 거버넌스의 공백은 법령과 규정에 의해 어느 정도 해결되고 있습니다. 1990년대 후반과 2000년대 초에 발생한 일련의 재무보고 스캔들에 대한 대응으로 2002년에 제정된 사베인스-옥슬리 법은 이러한 의무 중 일부는 감사위원회에 속한다는 것을 명확히 하였습니다. 구체적으로, 사베인스-옥슬리 법을 시행하는 SEC(증권거래위원회)의 10A-3 규칙은 "감사위원회는 회계, 회계통제 또는 감사에 관한 문제사항을 접수, 보존 및 처리하기 위한 절차를 수립하여야 하며, 의문스러운 회계 또는 감사사항에 대한 우려를 기밀로 익명 제출할 수 있도록 해야 한다"고 명시합니다. 그 결과, 핫라인을 보유하지 않았던 상장법인들은 핫라인을 도입하고 특정 불만 및 우려사항을 감사위원회에 보고하도록 권고받았습니다.

초기에 회계 및 감사사항을 처리하기 위해 도입된 핫라인은 점차 임직원의 다양한 문제를 다루는 저장소로 자리매김하게 되었습니다. 윤리강령 위반, 근무 환경, 일반적인 불만과 제안 등 다양한 주제를 아우르게 되었습니다. 그러나 회사 내에서 비감사 및 회계사항에 대한 별도 보고 프로세스를 개발하는 대신, 많은 회사에서는 감사위원회가 이러한 사항에 대한 보고를 받았으며 현재까지도 그 역할을 수행하고 있습니다. 결과적으로 감사위원회는 직원들의 다양한 불만과 우려사항에 대한 궁극적인 거버넌스 감독 기능을 수행하고 있습니다.

감사위원회의 책임 및 자원

감사위원회는 이러한 사안에 궁극적인 감독 책임을 보유하고 있을 수 있지만, 컴플라이언스 및 윤리와 관련된 책임 이외에도 다른 광범위한 책임을 갖고 있습니다. 따라서 감사위원회는 특정 컴플라이언스 영역을 감독하기에 적합한 위원회인지를 고려해야 합니다. 예를 들어, 금융 및 회계 사항과 관련되지 않는 특정 유형의 리스크는 보상위원회 또는 임원후보추천/거버넌스위원회가 더 적합한 감독을 수행할 수 있습니다. 이를 통해 감사위원회는 주요 리스크 관리 감독과 직접적으로 관련된 사안에 자원을 집중할 수 있습니다.

감사위원회는 또한 컴플라이언스 및 윤리와 관련된 정보를 받고 검토하는 절차에 대해서도 고려할 수 있습니다. 예를 들어, 많은 회사에서 감사위원회는 핫라인 보고서를 받는 유일한 이사회 수준의 위원회입니다. 그러나 제출된 보고서의 건수가 많고, 감사위원회의 감독 영역과 관련이 없는 경우, 감사위원회는 심각도나 관련성과 같은 기준을 충족하는 보고서만 선별적으로 검토할 수 있습니다. 이 경우, 감사위원회는 중요한 보고서가 누락되지 않도록 관리 담당자에게 책임을 위임하거나 다른 위원회나 경영진에게 제출된 사안이나 동향에 대해 감사위원회에 보고할 책임을 부여할 수 있습니다.

groups, such as customers or vendors. (It is important to note, however, that the audit and other committees should not necessarily treat as good news the receipt of few submissions or a decline in the number of submissions. This may indicate technical problems that make it difficult to access the hotline, poor communications about its availability or purpose, or lack of trust among employees.)

The audit committee needs to be aware of, and make appropriate use of, all of the resources available to it in connection with its ethics and compliance oversight role. Perhaps the most important resource is the company's compliance function, which typically performs a critical role in aggregating and reporting to the audit committee on the overall performance and effectiveness of the ethics and compliance program. Another resource may be internal audit (IA). For companies that have an IA function, it can be used in a variety of ways, such as analyzing data, developing standard protocols for following up on ethical or compliance concerns, or assessing whether the company's internal controls need to be enhanced to capture ethical or compliance breaches. IA can also work with a wide variety of functions both within and outside the company to assist committees in overseeing these areas. Other resources available to audit committees include internal and external counsel, investigators, consultants, and others; a combination or "ensemble" of these resources can help the committee to bridge the gap when other resources may not be adequate.

Beyond these resources, the committee may need to consider new approaches, tools, and processes as the company evolves and grows.

Foundational elements—risk as a starting point for ethics and compliance oversight

The audit committee's remit with respect to ethics and compliance is broad and deep and may be difficult to address without a focus on the most important risks. Thus, the first questions that an audit committee might consider in overseeing compliance and ethics may include "What are the greatest areas of ethical and compliance risks we face?" "Are we looking at the right risks, and if not, what risks should we be looking at?"

The audit committee should consider its oversight of ethics and compliance in the context of the company's existing risk profile, including its enterprise risk management process and policies designed to address specific risks. However, relying upon existing processes and policies may not suffice, particularly for companies that have just become publicly held or are initiating a product/service or geographical expansion or other departures from historical businesses and operations. And even companies that are mature and/or relatively stable may benefit from a fresh look at the risks that need to be addressed. This fresh look can be implemented through a number of approaches, such as peer company benchmarking or evaluations or assessments conducted by independent third parties.

Increasingly, companies are also using data-driven risk assessments and monitoring. For example, the US Department of Justice issued guidance in late 2020 emphasizing this approach, in contrast to static, point-in-time risk assessment processes. If a company is not integrating "big data" into its compliance program, the committee may request management to introduce it to facilitate its oversight role.

Of course, in some areas, data-driven risk assessments and monitoring may generate unclear or ambiguous results; this may be the case in areas where technology and key performance indicators are still developing, such as compliance with policies to address climate change. Consequently, reliance on big data to the exclusion of other methods may be unwarranted or present additional risks from a completeness and accuracy perspective.

또한, 핫라인을 고객이나 공급업체와 같은 다른 이해관계자 그룹에 확대하여 사용하는 경우 전달의 측면에서 문제가 발생할 수 있습니다. 그러나 중요한 점은 감사위원회 혹은 다른 위원회가 제출된 보고서 수가 적거나 감소하는 것을 반드시 긍정적으로 받아들여서는 안 된다는 것입니다. 이는 핫라인에 접근하기 어려운 기술적인 문제, 핫라인의 가용성이나 목적에 대한 안내 미흡, 또는 직원 간 신뢰 부족 등을 보여주는 것일 수 있습니다.

감사위원회는 윤리 및 컴플라이언스 감독 역할과 관련하여 활용 가능한 모든 자원을 알고 적절하게 활용해야 합니다. 회사의 컴플라이언스 기능은 일반적으로 가장 중요한 자원으로 여겨지며, 윤리 및 컴플라이언스 프로그램의 전반적인 성과와 효과에 대한 정보를 종합하여 감사위원회에 보고하는 역할을 수행합니다. 내부감사도 다른 자원으로 활용될 수 있습니다. 내부감사 기능을 갖춘 회사의 경우, 데이터 분석, 윤리 및 컴플라이언스 관련 문제에 대한 후속 조치를 위한 표준 프로토콜 개발, 또는 윤리 및 컴플라이언스 위반을 파악하기 위해 회사의 내부통제를 강화해야 할 필요성을 평가하는 등 다양한 방식으로 활용될 수 있습니다. 내부감사는 회사 내외의 다양한 부서와 협력하여 감사위원회가 이러한 영역들을 감독하는 데 도움이 될 수 있습니다. 감사위원회가 활용할 수 있는 또 다른 자원으로는 내부 및 외부 법률자문, 조사관, 컨설턴트 등이 있으며, 이러한 자원들의 조합은 다른 자원이 충분하지 않을 때 감사위원회가 자원의 공백을 메우는 데 도움이 될 수 있습니다.

이러한 자원들 이외에도, 회사가 진화하고 성장함에 따라 감사위원회는 새로운 접근 방식, 도구 및 프로세스를 고려해야 할 수도 있습니다.

기본 요소 – 윤리와 컴플라이언스 감독을 위한 시작점으로서의 리스크

감사위원회의 윤리 및 컴플라이언스에 대한 역할은 광범위하고 심도 있으며, 가장 중요한 리스크에 초점을 맞추지 않으면 해결하기 어려울 수 있습니다. 따라서 감사위원회가 컴플라이언스 및 윤리를 감독하는 과정에서 고려해야 할 첫 번째 질문은 "우리가 직면한 가장 큰 윤리 및 컴플라이언스 리스크 영역은 무엇입니까?"와 "우리는 올바른 리스크를 살펴보고 있는지, 그렇지 않다면 어떤 리스크를 살펴봐야 합니까?"가 될 수 있습니다.

감사위원회는 회사의 기존 리스크 프로파일을 고려하여 윤리 및 컴플라이언스 감독을 수행해야 합니다. 이는 기업의 리스크 관리 프로세스 및 특정 리스크를 해결하기 위해 마련된 규정을 포함합니다. 그러나 기존의 프로세스와 규정에 의존하는 것만으로는 충분하지 않을 수 있습니다. 특히 공개적으로 거래되는 기업이나 제품/서비스나 지역적 확장 또는 기존 사업 및 운영방식에서 벗어나는 기업의 경우에는 더욱 그렇습니다. 또한 성숙하거나 비교적 안정적인 기업도 새롭게 고려해야 할 리스크를 살펴보는 것이 유익할 수 있습니다. 이러한 새로운 관점은 경쟁사 벤치마킹이나 독립적인 제3자에 의한 평가와 같은 다양한 방법을 통해 구현될 수 있습니다.

최근에는 점차 더 많은 기업들이 데이터 기반의 리스크 평가 및 모니터링을 활용하고 있습니다. 예를 들어, 미국 법무부는 2020년 말에 정적이고 특정 시점에서만 이루어지는 리스크 평가 프로세스와는 대조적인 이 접근 방식을 강조하는 지침을 발표하였습니다. 회사가 "빅데이터"를 컴플라이언스 프로그램에 통합하지 않고 있다면 감사위원회는 경영진에게 이를 도입하여 감독 역할을 원활히 수행할 수 있도록 요청할 수 있습니다.

물론 일부 영역에서는 데이터 기반 리스크 평가 및 모니터링이 명확하지 않거나 모호한 결과를 초래할 수 있습니다. 특히 기후변화와 관련된 규정의 준수와 같이 기술 및 핵심 성과 지표가 아직 개발중인 영역에서는 이런 경우가 발생할 수 있습니다. 따라서 다른 방법을 배제하고 빅데이터에만 의존하는 것은 완결성 및 정확성 측면에서 무분별하거나 추가적인 리스크를 초래할 수도 있습니다

Next steps and the critical importance of employee communications

Assuming that the relevant risks have been identified, the committee should seek management's assistance in determining whether the company's ethics and compliance policies, processes, and procedures optimally address those risks. The following are some of the key questions the audit committee can ask about the company's ethics and compliance policies:

- Do we have the right policies in place? Are there key risks for which we don't have policies?
- Have existing policies been updated to address recent developments, including changes in the company, in law or regulation, and otherwise?
- Do we have the right management resources to monitor and enforce compliance with our policies? How are we using technology to monitor and enforce our policies?

Again, peer company benchmarking and independent evaluations and assessments can be useful tools in addressing these areas.

However, even the best policies, processes, and procedures may not succeed if the company is unable to get its employee communications "right." To be effective, communications need to attract and retain employees' attention, and companies need to determine whether their communications are achieving these goals and making their messages "sticky." The dramatic increase in hybrid and remote work arrangements in the current environment has complicated these challenges at the same time that it may lead to heightened incidence of fraud.

Wrapping it up

The importance of corporate ethics and compliance is not diminishing; if anything, given the current focus on environmental, social, and governance issues and a growing focus on corporate responsibility and so-called "stakeholder capitalism," it seems likely that ethics and compliance will continue to grow in importance. Consequently, audit committees will likely need to maintain or increase their oversight efforts of these matters. In that environment, it is important that audit committees view their ethics and compliance responsibilities holistically, taking into account the above and other factors, maintain an open posture to keep what is working, and consider new approaches as needed.

향후 단계와 직원 커뮤니케이션의 중요성

관련 리스크 요소가 파악되었다는 전제 하에, 감사위원회는 회사의 윤리 및 컴플라이언스 규정, 프로세스가 해당 리스크를 최적으로 다루는지 여부를 판단하기 위해 경영진의 도움을 요청해야 합니다. 다음은 감사위원회가 회사의 윤리 및 컴플라이언스 규정에 관해 물어볼 수 있는 주요 질문들 입니다.

- 적절한 규정을 보유하고 있습니까? 규정이 없는 주요 리스크 요소가 있습니까?
- 최근의 회사의 변화, 법률 또는 규정의 변화 등을 고려하여 기존 규정이 업데이트되었습니까?
- 규정의 준수를 모니터링하고 시행하는 데 필요한 적절한 경영 자원을 보유하고 있습니까? 기술을 어떻게 활용하여 규정 준수를 모니터링하고 시행하고 있습니까?

경쟁사 벤치마킹, 독립적인 평가 및 측정은 이러한 영역을 해결하는 데 유용한 도구일 수 있습니다.

그러나 회사가 직원들의 커뮤니케이션을 "적절하게" 이루어지도록 할 수 없다면 아무리 좋은 규정, 프로세스 및 절차도 성공하지 못할 수 있습니다. 커뮤니케이션이 효과적이기 위해서는 직원들의 관심을 끌고 유지할 수 있어야 하며, 회사는 자사의 커뮤니케이션이 이러한 목표를 달성하고 메시지가 "잘 전달되는지" 확인해야 합니다. 또한, 현재의 하이브리드 및 재택근무의 확대 상황은 커뮤니케이션 문제가 복잡해짐에 따라 부정행위의 발생을 증가시킬 수도 있습니다.

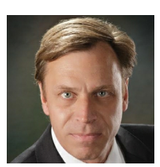
마무리하며

기업의 윤리 및 컴플라이언스의 중요성은 줄어들지 않고 있습니다. 현재 환경에서는 환경, 사회, 지배구조 문제에 대한 관심이 커지고 기업의 책임과 "이해관계자 자본주의"가 주목받으면서, 윤리 및 컴플라이언스의 중요성은 계속해서 커질 전망입니다. 따라서 감사위원회는 이러한 문제들에 대한 감독 노력을 유지하거나 강화해야 할 것으로 예상됩니다. 이러한 환경에서 감사위원회는 윤리 및 컴플라이언스 책임을 종합적으로 고려해야 합니다. 앞서 언급한 사항 뿐 아니라 다른 요소들을 고려하고 기존의 효과적인 접근방식을 유지하고, 필요에 따라 새로운 접근방식을 고려해야 합니다.

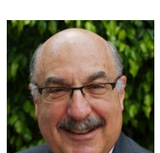
On the audit committee's agenda | US

저자

Krista Parsons
Managing Director and
Audit Committee Program Leader
Center for Board Effectiveness
Deloitte & Touche LLP
kparsons@deloitte.com



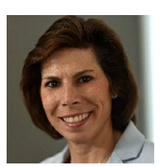
Robert Biskup
Managing Director
Regulatory, Forensics & Compliance
Deloitte & Touche USA, LLP
rbiskup@deloitte.com



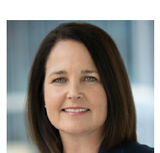
Bob Lamm
Independent Senior Advisor
Center for Board Effectiveness
Deloitte LLP
rlamm@deloitte.com

문의

Carey Oven
National Managing Partner
Center for Board Effectiveness
Deloitte & Touche LLP
coven@deloitte.com



Maureen Bujno
Managing Director and
Audit & Assurance Governance Leader
Center for Board Effectiveness
Deloitte & Touche LLP
mbujno@deloitte.com



Audrey Hitchings
Managing Director
Executive Networking
Deloitte Services LP
ahitchings@deloitte.com

Caroline Schoenecker
Experience Director
Center for Board Effectiveness
Deloitte LLP
cschoenecker@deloitte.com

기업지배기구발전센터 Contact

김한석 센터장
Partner / Audit & Assurance,
Center for Corporate Governance Leader

김학범 파트너
Partner / Risk Advisory

정 현 파트너
Partner / Audit & Assurance

오정훈 파트너
Partner / Audit & Assurance

About this publication
This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About the Center for Board Effectiveness
Deloitte's Center for Board Effectiveness helps directors deliver value to the organizations they serve through a portfolio of high quality, innovative experiences throughout their tenure as board members. Whether an individual is aspiring to board participation or has extensive board experience, the Center's programs enable them to contribute effectively and provide focus in the areas of governance and audit, strategy, risk, innovation, compensation, and succession. For more information, contact us at centerforboardeffectiveness@deloitte.com.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (DTTL), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US members firms of DTTL, their related entities that operate using the "Deloitte" name in the United States, and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2023 Deloitte Development LLC. All rights reserved.