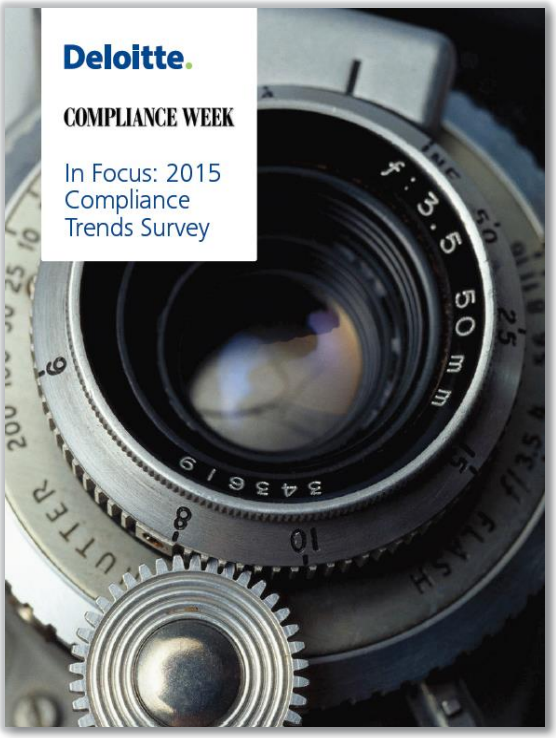
Deloitte. THE WALL STREET JOURNAL.

본 기사는 美 THE WALL STREET JOURNAL에 발간된 Deloitte의 영문 기고문을 번역하여 연재한 자료입니다.

Third parties 리스크 관리: CCO의 최우선 과제

딜로이트와 컴플라이언스 전문지 Compliance Week[1]의 공동 서베이(In Focus: 2015 Compliance Trends) 결과에 따르면, Third parties와 그들이 제기하는 위험은 조직 컴플라이언스 문화 구축과 함께 CCO[2]의 가장 큰 도전 과제로 선정되었습니다.

서베이는 연간 매출액 10억~50억 달러인 기업에서 윤리, 준법 감시, 감사, 리스크 관리 또는 기업지배구조 분야에 종사 중인 364명의 고위 경영진의 응답을 토대로 한 것입니다. 서베이 응답자들은 Third parties를 직면하고 있는 가장 어려운 문제로 꼽았으며, 이를 관리하기 위하여 아래와 같이 나열하였습니다.



- 정책이나 규정 준수 상시 감사(42%)
- 광범위한 백그라운드 상시 조사 수행(38%)
- 교육이나 인증 상시 요구(32%)

또한, 설문에 "때때로(Sometimes)"라고 답한 응답자까지 포함할 경우, 전체 응답자의 70%가 Third parties에 어려움을 겪고 있는 것으로 나타났습니다.

중앙 집중식 컴플라이언스 기능에 대한 CCO의 컴플라이언스 책임은 회사마다 다르지만, 여전히 몇 가지 핵심적인 책임이 지배적입니다. 해당 서베이에서는 컴플라이언스 교육(76%), 행동 강령(74%), 내부 고발자 핫라인(70%), 규제 및 내부 Compliance 조사(68%), 이해관계 충돌(68%) 등이 공통 책임으로 나타났으며, 하위 책임 영역으로는 규제 관계 관리(40%), 자금 세탁 방지 프로그램(40%), 기록 및 정보 관리(36%), 커뮤니케이션(35%), 문화 평가(24%) 등이 도출되었습니다.

귀사에서 컴플라이언스 기능은 어느 영역을 담당합니까?

Top five answers

- 76% Compliance 트레이닝
- 74% 행동강령
- 70% Complaints 및 내부고발자 핫라인
- 68% 규정 및 내부 Compliance 조사
- 68% 이해관계 충돌

Bottom five answers

- 40% 규제관계관리
- 40% 자금 세탁 방지 프로그램
- 36% 기록 및 정보 관리
- 35% 커뮤니케이션
- 24% 문화 평가

[1] Compliance Week는 윌밍턴 그룹(Wilmington Group)에 의해 미국 보스턴에서 2002년 창간된 기업지배구조, 리스크 및 윤리·준법 경영 관련 전문 언론지

[2] 최고준법책임자(Chief Compliance Officer, CCO)는 기업의 준법적이고 윤리적인 조직 문화를 유지하기 위해 이를 감독할 책임이 있는 경영진이다.

문화 평가(Culture Assessments) : 중요하지만 부족한 오너십

문화 평가는 지난해(`14년)의 26%에서 더욱 감소한 24%로 2년 연속 CCO의 하위 기능을 차지했습니다. Mohlenkamp는 효과적인 컴플라이언스 프로그램을 개발하기 위해선 기업 문화에 대한 날카로운 이해가 중요하다고 강조합니다. 다만, 조직 모든 사람의 이해를 필요로 하기 때문에, '컴플라이언스가 문화를 소유(compliance owns culture)'한다거나 'HR이 문화를 소유(HR owns culture)'한다와 같이 역할을 정확하게 정의할 수는 없으며, 많은 조직에서 아무도 이를 평가할 책임을 지지는 않는다라고 덧붙였습니다. 문화를 평가해야 할 마땅한 두 집단은 컴플라이언스와 HR입니다. 그러나 그들은 어떻게 해야 실행 가능한 결과를 만들어낼 수 있을지 모를 것입니다. 서베이 응답자의 55%는 CCO가 이사회와 CEO에게 "윤리 및 문화에 대한 일반적인 보고서"를 제공한다 답했습니다. 그럼에도 불구하고, 조직이 문화를 충분히 평가하지 않는다면, 이는 '행동 수칙'과 '내부 고발자 보복에 관한 준법 교육' 등과 같은 CCO의 주요 우선순위를 위험에 빠뜨릴 수 있습니다.

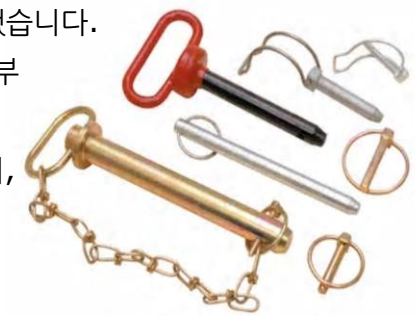
리스크 평가(Risk Assessments) : 컴플라이언스 리스크 관리를 위한 린치핀(Lynchpin)[1)]

응답자의 80% 이상이 전사적 컴플라이언스 위험 평가를 수행한다고 답하였으며, 64%가 높은 빈도로 수행하지는 않더라도 적어도 매년 평가를 실시한다고 답했습니다. 또한, 기업의 컴플라이언스 위험 평가를 수행하는 방법은 1) 독립 실행, 2) 내부 감사 위험 평가의 일환으로 수행, 3) 일반 기업 위험 평가의 일환으로 수행이 동일하게 각 33%의 응답률로 나뉘었습니다.

Deloitte & Touche LLP의 Deloitte Advisory Director인 Tom Rollauer와 Deloitte 규제전략센터 Executive Director는 "위험 평가는 컴플라이언스 위험을 관리하는 노력의 중심에 있다"라고 말하며, "만약 귀사가 강력한 전사적 위험 평가 프로세스를 가지고 있다면, 귀사의 우선순위는 그것으로부터 발전할 것이며, CCO는 이러한 위험 평가를 기반으로 규정 준수 모니터링 및 테스트 우선순위를 설정해야 한다."라고 말했습니다.

Tom Rollauer는 또한 이러한 유형의 프로세스를 시행해 온 조직들은 비교적 이를 잘 활용하는 편이며, 프로세스를 이제 막 구현해보는 이들은 선진적이지 않을 수 있고 제대로 이행하지 못할 수도 있으나, **'결국 컴플라이언스 프로그램의 효과는 위험 평가 프로세스의 성숙도와 품질에 기초한다'**라고 말했습니다.

Deloitte Financial Advisory Services LLP의 Deloitte Advisory의 Director인 Biegelman는 기관들이 컴플라이언스 부서를 넘어서 위험 평가를 실시할 것을 권장했습니다. 그는 "일반적으로 컴플라이언스 부서가 위험 평가를 실시함에 있어 내부 감사와 긴밀히 협력하는 것은 좋은 일입니다"라고 말했습니다. 하지만 그는 "비즈니스 부서의 의견을 얻는 것도 중요하다"라 강조하며, ***"리스크 평가 과정에 대한 비즈니스 리더의 참여와 피드백이 없다면 확인된 리스크를 해결하는 것이 더욱 어려울 수 있다"***라 지적합니다.



[1)] 린치핀(Lynchpin)이란 마차나 수레의 축에 위치한 핀으로, 핵심축이라는 의미로 중요한 역할 또는 필요한 인물을 의미한다.

** Image source: shutterstock, different types of pins for tractors and trailers

Deloitte. THE WALL STREET JOURNAL.

Third parties 리스크 관리: 전사적 리스크 관리의 필요성

기업의 외부 업체 이용은 하루 이틀 이루어진 일이 아닙니다. 기업은 수년간 공급 업체, 아웃소싱 업체, 라이센스 업체, 대행업체 등과 협력해 왔습니다. 달라진 것은 Third parties 사용 빈도와 규모, 그리고 조직이 내재된 Third parties 리스크를 어떻게 관리하고 있는지에 대한 감독기관의 규제입니다.

영국 Deloitte LLP의 Contract Risk & Compliance 파트너인 Kristian Park는 Third parties 위험의 단계적 확대와 조직의 리스크를 완화 방법에 대한 이야기를 공유하였습니다.

Q: Third parties의 리스크가 커지는 이유는 무엇입니까?

Kristian Park

몇 가지 요인이 작용합니다.

그중 첫째는 '부피(Volume)'입니다. 경기 침체기 동안 많은 조직들은 내부 비용을 절감하기 위해 보다 많은 업무를 Third parties에게 맡기곤 했습니다. 당연히 부피가 커질수록 위험이 높아질 수밖에 없습니다.

두 번째는 '감독'입니다. 규제 당국이 점차 기업이 어떻게 아웃소싱 및 Third parties 리스크를 관리하는지 중점을 두기 시작하며, 관련 위반 건이 수억 달러에 도달하게 되었습니다.

그리고 이러한 요소들로 인해 세 번째 요소가 생겨나게 되었는데, 그것은 바로 '명성에 미치는 영향'입니다. 수백만의 소비자가 Third parties 시스템 오류 또는 보안 위반으로 인해 피해를 받게 되거나, 지명도가 높은 회사가 MRA(관심이 필요한 문제) 규제로 반복 언급되는 경우, 해당 기업의 명성이 훼손될 수 있습니다.

정보의 자유로운 유동성도 여기서 중요한 역할을 합니다. 수십 년 전, 도시의 논란은 그 도시에서만 머물곤 했습니다. 하지만 오늘날에는 전 세계적인 이슈가 되고는 합니다.

위험이 점차 증대 및 현실화되면서 이사회는 보다 더 많은 관심과 문제를 제기하게 됩니다. 사실상, 대부분의 선도적 글로벌 조직에서 조차도 회사의 비즈니스 파트너 혹은 Third parties가 가지고 오는 리스크에 대해 전반적인 이해를 하고 있는 사람은 거의 없습니다. 이는 극히 우려되는 일입니다. 이전과 달리, 오늘날의 이사회는 Third parties의 위험을 가장 높은 레벨의 전략적 리스크로 간주하고 있습니다. 그러나 Third parties 위험은 아직까지 단일 담당자 또는 단일 기능 부서의 명확한 책임으로 지정된 바 없습니다. 조달 담당자는 종종 Third parties 위험에 대한 역할(Role)을 수행하도록 요청받고는 하였지만, 이는 이해관계를 모두 고려한 전사적 관점이 아닌, 유통 파트너 등 만을 고려한 공급 분야에 편향되어 있는 관점입니다.

Q: Third parties 리스크 관리에 대한 전통적인 접근법은 무엇이며, 개선 가능한 부분이 있습니까?

Kristian Park

Third parties 위험은 일반적으로 고립된 방식으로 다루어져 왔으며, 조직의 개개인은 대개 공급망 내 특정 위험만을 살펴보았습니다. 예를 들어, 은행업에서는 IT 부서와 데이터 보호, Third parties와 데이터 공유 리스크에 중점을 둘 것이며, 소비자 제품 업계에서는 최종 소비자와 회사의 명성을 보호하기 위해 제품의 품질과 안전에 대한 위험에 중점을 둘 것입니다. 조직은 비즈니스 특징이나 기능적 층면에 대한 위험을 관리하는데 능동적인 반면, 좁은 관점에서 벗어나, 광범위한 리스크에 대한 노출은 검토하고 있지 않습니다.

전체론 적인(전사적인) 시야는 Third parties 및 기업 전사적 관리로부터 발생하는 리스크의 노출 결과를 이해하는 것에 있어 필수적이라 할 수 있습니다.

조직 내 서로 다른 레벨의 관리층에서 어떻게 다른 관점을 갖고 있는지 확인하는 것은 매우 흥미로운 일입니다. 예로, 조달 책임자는 Third parties 리스크가 통제되고 있다 말할 것이지만, 아래 직원들은 어쩌면 그처럼 100% 확신할 수 없을 수 있습니다. 그들은 이미 특정 위험 영역이 감추어지고 있다는 것을 알고 있습니다.

최고 경영인(C-suite)이나 이사회와 같은 상위 리더들은 대개 해당 문제에 대해 덜 낙관적으로, Third parties의 위험을 해결되지 않은 심각한 문제로 인식하고 있습니다.

Q: 선도적인 기업들은 Third parties 리스크 관리를 어떻게 수행하고 있습니까?

Kristian Park

많은 기업이 아직 여정 중에 있습니다. 그중 일부는 Third parties 리스크 관리를 위한 길로 더 나아가고 있지만, 여전히 많은 기업은 이러한 수준에 미치지 못하고 있습니다.

첫 번째 단계(Step)인 '비즈니스 파트너에 대한 가시성 확보'는 여정의 큰 걸림돌 역할을 하곤 합니다. 회사가 어느 정도 가시성을 갖게 되면, 그들은 자신이 식별한 Third parties 관련 리스크를 어떻게 관리할 것인가에 대해 생각을 시작하게 되며, 주로 가장 높은 리스크를 내포하고 있는 방면에 모든 노력을 집중하곤 합니다. 이는 전반적인 대응이라 하기보다는, 비례적인 대응이라 할 수 있습니다.

이를 위한 확실한 방법은 통상 Third parties 리스크 프레임워크와 정의된 프로세스(예: Third parties에 배포되는 설문지 및 응답을 기반으로 한 잠재적 리스크 평가 수단)를 포함합니다. 일단 위험이 식별되면, 이를 바로잡을 수 있는 강력한 거버넌스가 마련될 것입니다. 이 단계는 리스크를 바로잡을 가이드뿐 아니라, 리스크에 대한 수용 여부와 어떻게 하면 올바르게 리스크를 관리할 수 있는지에 대한 내용들이 포함되며,

Third parties 리스크와 리스크 관리 백그라운드를 가진 조직 내의 사람은 이에 대한 명확한 소유권을 갖게 될 것입니다.

우리는 이러한 단계를 거친 조직들을 많이 보았습니다. 통상적으로 기업이 전사적 범위에서 이를 구현하는 데 있어서 가장 걸림돌이 되는 것은 기술적인 한계입니다. 심지어 스프레드시트로 이를 관리하려 하는 글로벌 기업까지 볼 수 있었습니다. 하지만 사실은 이를 해결하기 위한 기술적 솔루션이 존재하지 않아서가 아닙니다. 단지 이를 위해서는 기업의 많은 노력과 비용이 필요하기 때문입니다. 이러한 것들은 많은 기업의 발목을 잡고 있습니다.

Deloitte. THE WALL STREET JOURNAL.

Third parties 리스크 관리: 가치 창출 및 보호

Third parties 관계는 주주 가치에 부정적이거나 긍정적인 영향을 미칠 수 있는 힘을 가지고 있으며, 공급 업체가 제공하는 서비스의 규모와 유형에 기하급수적인 영향을 미칠 수 있습니다. Third parties 리스크 관리의 초점은 단점을 보완하기 위하여 조직을 보호하는 데 있는 경우가 많지만, 확장된 엔터프라이즈에서 Third parties 리스크를 능동적으로 관리하는 조직은 생산성 향상, 계약 및 자산 최적화, 유연성 향상, 성장 기회 확대 등 여러 가지 이점을 얻을 수 있습니다.

일반적으로 Third parties는 고객, 파트너, 대리인, 벤더 및 서비스 제공자를 포함하여 회사가 사업을 하는 개인 또는 기업을 말합니다. 한마디로 세계 각지에 위치한 이러한 Third parties들이 "확장 엔터프라이즈(이하, 확장된 기업)"를 구성하게 됩니다. 확장된 기업이 성장하고 더욱 복잡해짐에 따라, 조직은 전략적이고 주동적으로 Third parties 행동에 대한 노출을 관리하는 것을 고려해야 합니다.

문제는 리스크 관리가 분열 및 분산되는 경우가 많고, 리스크 관리에 대한 집중도가 높아지고 있음에도 불구하고 일부 조직에는 여전히 리스크 전담 담당자가 없다는 점입니다. 또한, 일부 조직에서는 여전히 확장된 기업 전반에서 위험관리와 성과 달성을 관리하기 위한 '3가지 방어선(사업 단위, 거버넌스, 내부감사)'를 어떻게 활용할지 충분하게 고려하지 않는다는 점입니다.

Krissy Davis

Deloitte & Touche LLP의 Deloitte Advisory 파트너인 Krissy Davis는 "많은 조직이 포인트 솔루션을 통해 임시적이고 선별적인 방식으로 Third parties 리스크 관리에 접근하고 있으며, 사이버 리스크와 규정 준수 의무 같은 중요한 문제를 발생 시 해결한다. " 라고 말했습니다. 또한 "소유권 부족이 공통의 테마인 가운데, 기업 간 폭넓은 견해가 누락되는 경우가 많다. 조직들은 가치 창출과 가치 보호를 강조하는 확장된 기업 위험 관리 프로그램(EERM)을 충분히 고려해야 한다."라고 지적했습니다.

분산된 위험 관리와 관련된 문제는 확장된 기업 전체의 비즈니스 목표 및 위험 영역과 위험 관리 구성요소를 연결하여 가치를 창출하는 효과적인 EERM 모델로 해결할 수 있습니다.

Dan Kinsella

Deloitte & Touche LLP의 Deloitte Advisory 파트너인 Dan Kinsella는 "EERM은 비즈니스 성과를 촉진하는 사전 예방적 지렛대가 될 수 있다. " 라고 말했습니다. Kinsella는 또한 "조직이 리스크 관리 프로세스를 활용하여 성능을 향상시키기 위해서는, 취약성이 사전에 해소될 수 있도록 확장된 기업 전체에 걸쳐 체계적으로 리스크를 감지하는 End-To-End 접근 방식을 개발하는 것이 중요하다."고 덧붙였습니다.

일부 조직은 전체 구조를 복구하는 것과 달리, 확장된 기업을 관리하는 데 '누수된 부분 패치'를 시도하려 합니다. 예를 들어, 그들은 공급업체의 위험 프로필, 통제 환경 및 성과를 이끌어 낼 수 있는 능력에 초점을 두기보다는, Third parties를 고용할 때 저비용의 공급자를 찾는 등 그들의 지출에 집중할 수 있습니다.

또한, 일부 조직에서는 확장된 기업에 대한 End-To-End 접근 방식을 취하는 것은 어려운 일입니다. 경영진의 지원을 확보하고, 사람들에게 책임을 갖게 하는 것이 매우 어려운 일이기 때문입니다. 또한, 일부 조직에선 이러한 과제가 너무 방대하다고 간주될 수 있으며, 포괄적인 Third parties 감독 프로그램을 구축, 실행 및 유지할 수 있는 경험과 자원이 부족하다 생각할 수 있습니다.

Davis는 "장애물은 현실보다 더 많은 지각(知覺)이다."라고 말합니다. 그는 "모든 것을 한 번에 할 필요도 없고, 할 수도 없다. EERM 프로그램을 수립하거나 기존 프로그램을 발전시키는 데 필요한 실질적인 단계를 확인하는 것이 오히려 중요한 문제다."라고 밝혔습니다. 조직은 전략 및 거버넌스, 인력, 프로세스 및 기술과 관련하여 EERM 역량이 얼마나 발전됐는지 고려하는 것을 통해 단계에 대한 이해를 할 수 있습니다.

효과적인 EERM을 위한 4가지 구성요소

① 전략과 거버넌스

조직은 Third parties 리스크 관리를 위한 공식 전략 및 거버넌스 모델을 마련하는 것을 고려해야 합니다. 또한 거버넌스 모델을 평가하여 위험 관리 기법을 가치 요인과 연계할 만큼 민첩하고 유연한 지 판단해야 합니다. Third parties 관계에서 중단점이 어디에 존재하는지 이해하고, 사전 평가 및 유지를 위한 사전에 정해진 수단을 갖는 방법을 고려하여야 합니다. 비즈니스 임원과 컴플라이언스 및 리스크 전문가 간의 격차를 줄이기 위한 모델도 적극적으로 모색하여야 합니다.

② 인력 구성요소

효과적인 EERM 프로그램은 관계, 컴플라이언스 및 규정의 적극적인 관리를 요구합니다. 예를 들어, 조직은 확장된 기업 전체에 걸쳐 Third parties 리스크 관리를 위한 전담 역할을 할당하고, 사업 단위, 거버넌스 및 내부 감사라는 세 가지 방어선을 조정 및 강화하는 것을 고려해야 합니다. 기업 차원에서 EERM의 경영진 오너십은 새로운 규제 요건에 대해 직원과 Third parties가 최신 상태를 유지하는 것과 마찬가지로 프로그램 개선에 중요한 역할을 합니다.

③ 효과적인 프로세스

조직이 Third parties 사고에 대응하거나 예방하려는 방법과 관련된 절차와 프로토콜은 확장된 기업을 형성하는 이벤트를 탐색하는 데 도움이 될 수 있습니다. 예를 들어, 조직은 전사적으로 리스크 관리 프로세스를 표준화 및 통합할 수 있으며, 보다 탄력적인 전략에서 비용 절감 및 운영 효율성

향상에 이르는 다양한 이점을 얻을 수 있습니다. 진화하는 기술, 시장 동향 및 파괴력은 Third parties 관계에 기회와 과제를 제시합니다. 따라서, 이러한 요소들을 모니터링하는 것은 관계의 성패와 조직의 전략적 목표를 달성하는 데 기여할 수 있을 것입니다.

또한 조직은 적절한 계약이 시행되고 있으며 Third parties가 기대치를 충족하고 계약상 약정을 준수하고 있는지 확인할 수 있습니다. 효과적인 EERM은 미래의 제공 모델의 적절성을 쉽게 평가할 수 있는 능력과, 경영진이 시스템을 구축하거나 구입하는 것뿐만 아니라 아웃소싱이나 인소싱에 대한 의사결정에 자신이 있는 여부를 결정할 수 있는 능력을 요구합니다.

④ 기술, 데이터 및 분석

고급 기술을 사용하여 정보에 입각한 결정을 내리려면, 조직이 액세스할 수 있는 데이터와 Third parties 관계에 대한 결정을 내릴 때 활용할 수 있는 기술 도구를 이해해야 합니다. 효과적인 EERM은 리더가 정보에 접근하여 실시간으로 의사결정을 내릴 수 있도록 하고, 그러한 결정을 뒷받침할 핵심 성과 지표를 감시하고 분석할 수 있어야 합니다.

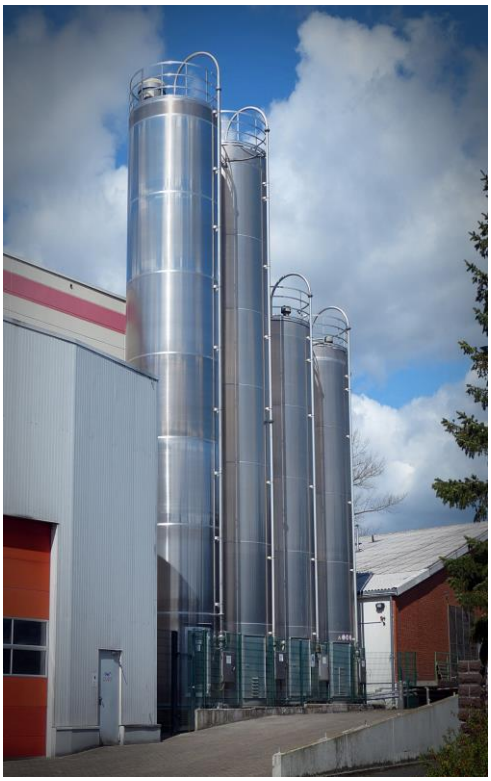
더 큰 기업 가치 추구

확장된 기업을 관리하기 위한 사전적인 노력은 조직이 다른 기업과 거래를 할 수 있도록 자격을 부여함으로써 수익 기회를 창출할 수 있습니다. 그러한 노력에는 공급자에게 국제 조약과 프로토콜을 준수하도록 요구하는 등 소싱 표준을 강화하는 조직이 포함될 수 있습니다. 구매자의 관점에서, 잘 정의된 공급자 표준은 거버넌스 프로세스 및 활성화 기술과 함께 공급망 컴플라이언스 최적화 프로그램의 중추를 형성할 수 있습니다. 이러한 프로그램은 Third parties의 정책 및 표준 준수를 도모할 뿐만 아니라 제품 품질 향상, 새로운 시장 진입, 지속 가능한 소싱에 대한 고객 요구 충족과 같은 회사의 광범위한 비즈니스 목표에 맞춰 확장된 기업을 조정함으로써 수익을 창출합니다.

Kinsella는 "복잡성과 자원 제약은 더 이상 확장된 기업에 통합적인 방법으로 Third parties 위험 관리를 피할 수 있는 충분한 이유가 되지 않으며, 미래에 대한 알 수 없는 두려움도 더 이상 되지 못한다."고 말했습니다.

Deloitte. THE WALL STREET JOURNAL.

Third parties 리스크 관리: 공급망 위험 평가



효과적인 공급망 위험 평가는 조직의 사일로[1]를 무너뜨리고, 경영관리 체계를 설정하여 이사회가 위험 방지 및 업무 중단 예방을 위한 전략을 세우는 데 도움이 될 수 있습니다.

평가 프로세스는 공급망과 마찬가지로 R&D, 제품 개발, 수요 및 공급 계획부터 제품 제조, 납품 및 고객 수익에 이르기까지 조직의 거의 모든 부분에 적용됩니다. 공급망의 범위와 역동적 특성은 위험 평가를 기업의 위험 관리의 중요한 요소로 만들었습니다.


James Cascone

Kate Ferrara

Deloitte & Touche LLP 파트너인 James Cascone과 Deloitte Global Food Value Chain 센터의 리더이자, Deloitte & Touche LLP 파트너인 Kate Ferrara는 공급망 위험 평가가 다른 평가와 다른 점, 시장이 조직의 평가 방법론에 어떤 영향을 미칠 수 있는지, 또한 어떤 평가 방법에서 인지 불가능한 잠재적 위험을 드러낼 수 있는지 논의했습니다.

Q: 공급망 위험 평가와 다른 종류의 위험 평가의 차이점은 무엇입니까?

James Cascone

공급망 위험 평가는 다른 조직과 크게 다릅니다. 많은 조직들은 공급망(예: 물류 공급업체)의 다양한 부분을 외부에 소싱하고 있으며, Third parties 리스크(예: 공급업체의 역량 혹은 재정적 가능성)에 대한 가시성이 제한됩니다. 공급망 글로벌화(소싱 및 제조 활동을 포함)의 특징은 새로운 위협을 도입한다는 것인데, 이는 연례 위험 평가에서 적시에 식별할 수 없을 가능성이 높습니다.

공급망은 역동적인 환경에서 운영되며 인터뷰 및 2차 연구와 같은 전통적인 방법을 사용하여 식별하고 모니터링하기 어려운 장애에 지속적으로 노출됩니다. 따라서 보다 능동적이고 예측적인 리스크 평가 프로세스가 필요합니다. 기업은 정기적으로 새로운 시장과 국가에 진출하거나, 문화를 혁신하거나 또는 정기적으로 새로운 제품을 출시할 수 있으며, 소매업과 같은 기업들은 제한된 프로모션을 제공할 수 있습니다. 비용, 성능, 그리고 리스크의 관점에서, 이러한 비즈니스 의사결정은 전체 공급망에 상당한 영향을 미칠 수 있습니다.

[1] 사일로(Silos)란 곡식을 저장하는데 이용되는 굴뚝 모양의 저장탑으로, 부서 간 서로 교류하지 않고 내부적 이익만을 추구하는, 독립성이 강한 부서를 뜻함

** Image source: pxhere, https://pxhere.com/ko/photo/1042807

Q: 공급망 리스크에 대한 전략적 평가 과정은 일반적으로 어디에서 시작되며, 누가 이를 주도하는가?

Kate Ferrara

회사 차원의 전반적인 전략과 공급망 조직 자체의 전략 두 가지 시작점이 있습니다.

전반적인 전략에는 고객 경험과 관련된 목표가 포함되며, 그중 상당 부분은 공급망 조직에 달려 있습니다. 특히 정확한 제품이 적합한 조건에 고객에게 전달되도록 보장할 수 있어야 합니다.

공급망 전략은 기업의 사회적 책임, fill rates, 시장 속도 및 제공 지표(delivery metrics)와 관련하여 서로 다른 목표를 가지고 있습니다. 예를 들어, 조직이 99%의 fill rates을 가지고 있는 경우, 공급망 기능은 회사가 fill rates을 달성하지 못하게 하는 위험에 초점을 맞출 것입니다.

James Cascone

공급망 위험이 궁극적으로 재무 성과에 영향을 미치기 때문에 대부분의 경우에 CFO가 평가를 주도하고 있습니다. 이는 또한 지속 가능성 또는 컴플라이언스 부문의 경영진들에 의해 주도될 수도 있습니다. 일부 조직에서는 리스크 관리, 내부 감사 또는 공급망 담당 부사장이 평가를 수행할 수도 있습니다. 이는 기업의 산업, 문화, 규모 등에 따라 상이합니다.

Q: 공급망 위험 평가를 방해하고, 역으로 지원할 수 있는 것은 무엇이 있습니까?

Kate Ferrara

많은 회사들이 사일로(silo)에서 공급체인을 관리합니다. 결과적으로, 단일 기능 내의 위험은 그 영역에서 일하는 사람들에게는 매우 높게 보일 수 있지만, 넓은 관점에서 볼 때, 이러한 위험은 최우선 관심사가 아닐 수도 있습니다.

전사적 관점은 전사적 차원에서 기업의 비즈니스 모델이나 전략에 영향을 미칠 수 있는 위험 영역에 관리자를 집중시키는 데 도움이 되기 때문에 중요하다고 할 수 있습니다.

James Cascone

공급망을 별개로 보아서는 안됩니다. 경영진의 견해가 단지 소싱이나 유통의 관점에서만 이루어진다면, 조직은 R&D, 신제품 개발과 관련된 가치사슬의 상류에서 비롯되는 몇 가지 핵심 이슈들을 다루지 않을 것입니다. 예로 마케팅 조직이 예정보다 빠른 시일 내 새로운 제품을 출시하려 하지만, 공급망 관련 조직과 커뮤니케이션을 하지 않는다면 부정확한 예측의 결과를 야기하여 현재의 공급 업체로 수요를 충족시키지 못할 수도 있습니다.

또한, 제품을 타겟 시장에 배포하기 위해 소요되는 공급 및 리드 타임이 존재할 수 있으므로, 부서 간 의사소통 및 협업을 장려하는 것은 무엇보다 중요합니다.

Q: 변화하는 비즈니스 환경이 공급망 위험에 접근하는 방식에 어떤 영향을 미쳤습니까?

Kate Ferrara

지난 10년 동안 컴플라이언스 문제, 기술, 세계화 등 많은 변화가 있었습니다. 이러한 맥락에서, 조직은 위험 상황 모니터링에 대한 사고를 할 때, 과거에 비해 통제할 수 없는 것들이 더 많아졌음을 깨닫게 될지도 모릅니다. 위험 감지 데이터는 이러한 상황에서 역할을 발휘합니다. 위험 감지 데이터는 조직에 어떤 상황이 발생할지 이해할 수 있도록 도움이 될 수 있기 때문입니다. 이러한 방법을 통해, 회사는 사건이 발생한 후 대응하는 것이 아니라, 보다 효과적으로 공급망 문제와 잠재적인 중단 또는 위험을 예상할 수 있게 됩니다. "어떻게 하면 발생할 수 있는 문제에 대해 더 잘 처리할 수 있을까?"라고 되묻는 것이 바로 해당 방법론을 시작하는 방법입니다.

Q: 공급망 위험 평가를 통해 밝혀진 예기치 않은 발견은 무엇이 있습니까?

James Cascone

일부 조직은 그들의 1차 공급 업체에 대한 가시성을 확보하고 있음에도 불구하고, 해당 공급업체들이 하고 있는 작업에 대해 그다지 투명성을 보유하고 있지 않고, 2차 또는 3차 공급업체가 무엇을 하고 있는지에 대하여는 전혀 알고 있는바가 없다는 사실에 놀랐습니다. 예를 들어, 일부 회사들은 공급자들이 재고 관리 방법을 알지 못했거나, 공급 업체의 생산 능력에 대한 확실한 알고있는 바가 없다는 것을 발견했습니다. 기업과 공급 업체는 종종 두터운 신뢰 관계로 이루어져 있지만, 위험 평가는 그 관계를 서서히 검증을 통한 접근 방식으로 변화시키고 있습니다. 공급망 위험 평가를 통해, 회사의 경영진은 특정 공급 업체의 진정한 취약점이 무엇인지 파악할 수 있으며, 공급 업체와 협력하여 보다 유연한 공급망을 개발할 수 있게 됩니다.

Q: 리스크 평가에서 Third parties 또는 조직 내부 공급망의 취약성이 확인되는 경우, 다음 단계는 무엇인가?

Kate Ferrara

평가의 일부는 기존 제어 컨트롤에 대한 더 나은 프로세스를 삽입하고 컨트롤과 프로세스를 공식화하는 것입니다. 일반적으로 더 포괄적인 관점에서 개발된 위험 우선순위 목록에 초점을 맞출 수 있는 중앙관리식 통제가 필요합니다. 경우에 따라 조직에서는 식별된 위험 각각에 소유자를 배정하고 그 사람에게 그러한 위험을 관리하거나 완화하기 위한 계획의 개발을 주도하도록 요구해야 합니다. 또한 소유주들은 일반적으로 조직이 잠재적 위험과 이를 다루는 방법에 대한 유용한 통찰력을 얻고 있는지 확인하기 위해 정기 보고서를 준비해야 합니다. 보고서에는 대시보드나 보드 레벨의 프레젠테이션에 사용되는 정보가 포함될 수 있으며, 평가 가치는 조직 현재 상태에 대한 정보를 제공하고, 프로세스 중에 식별된 위험을 수정, 설명 및 관리하는 데 도움이 됩니다.

Q: 실시간 감지 데이터가 공급망 위험을 모니터링하는 데 어떻게 도움이 될 수 있으며, 고려해야 할 요인은 무엇입니까?

James Cascone

조직은 매일 감지 데이터를 사용하고, 결과를 분석 및 해석하여 실시간으로 이상 보고서를 작성할 수 있습니다.

이런 식으로, 매일, 연속적으로 공급망 내의 잠재적 위험에 대한 감지 데이터를 분석하고 있습니다. 감지 데이터가 회사 정의에 따라 문제를 높은 위험 수준으로 이슈 제기하는 경우, 이메일이나 문자 메시지를 통해 즉시 경영진에 알립니다. 또는 주간 대시보드 업데이트의 일부로 데이터를 제공할 수도 있습니다. 모니터링할 문제점을 결정할 때 조직은 활용할 수 있는 다양한 데이터 소스, 해당 섹터에 관여하는 다양한 규제 기관 및 감시하고자 하는 국가를 고려해야 합니다.

또한 경영진은 회사가 위험 감지 중 자연어 처리 기술을 사용할 때 집중해야 할 주제에 대해 생각할 수도 있습니다. 그 예로 외식업계의 경우, 다른 산업에는 적용되지 않는 식량 재배에 사용되는 성분이나 화학물질과 관련된 핵심 문구나 기술적인 단어가 있을 수 있습니다. 이 경우 기업은 특정 용어를 센싱하고, 잠재 리스크가 중단의 결과를 초래하기 이전에 해당 리스크를 해결할 수 있습니다.

Q: 공급망 위험 이슈는 일반적으로 이사회 수준까지 올라가는가? 그렇지 않다면, 그렇게 해야 하는가?

Kate Ferrara

조직이 추구하고자 하는 전략을 추구하고, 이사회 차원의 관점에서 공급망 리스크를 바라보는 것이 가장 이상적입니다. 사실 현실은 일반적으로 이런 모습은 아니나, 현재는 변화 단계에 있습니다. 이사회가 직면해야 하는 많은 기타 이슈들을 고려할 때, 그들의 과제에 공급망 위험을 추가하는 것은 실현 가능하지 않을 수 있습니다. 그럼에도 불구하고, 경영진은 그러한 위험이 발생하기 전에 공급망 위험에 대한 논의를 더 전략적인 수준으로 격상시키는 방법을 고려해야 할 것입니다.

Resources

- 'Third-party Risks and Compliance Culture: CCOs' Top Challenges', The Wall Street Journal, February. 2016.
- 'Third-party Risk Management: Building a Robust Approach', The Wall Street Journal, December. 2015.
- 'Managing Third-party Risks to Create and Protect Value', The Wall Street Journal, March. 2016.
- 'Supply Chain Risk Assessment: Mining for Potential Threats', The Wall Street Journal, April. 2015.