Deloitte.

윤리경영, 디지털 기술의 적용

딜로이트 안진회계법인
FA Financial Crisis
김성일 부장

September 2019

윤리경영, 디지털 기술의 적용

들어가며

국내 제약·바이오 업계의 윤리경영 정착 및 확대와 관련하여 큰 흐름 2가지를 생각해 볼 수 있다. 첫 번째는 2018년 1월부터 시작된 경제적 이익 지출보고 작성 및 보관 제도[1]이며, 두 번째는 ISO37001 도입 및 인증의 추진이다. 법적 요구사항인 지출보고 작성 및 보관 제도가 외부환경 변화에서 촉발된 것이라면, ISO37001은 회사들의 자발적 도입이라는 차이가 있으며, 해당 변화는 제약·바이오 업계의 윤리경영 정착에 긍정적인 신호라 할 수 있다.

이에 본고에서는 윤리경영 정착에 있어 중요한 흐름인 ISO37001에 대해 알아보고, 특히 리스크 평가와 모니터링의 중요성을 언급하고자 한다. 더불어 번역본으로 제공된 딜로이트 글로벌 보고서, "제약 회사 컴플라이언스에서 가치를 유지하기 (Maintaining Value in Pharmaceutical Compliance)"에서 말하는 디지털 기술 우선 적용이 가능한 영역 또한 해당 영역임을 짚어봄과 동시에 마지막으로 리스크 평가와 모니터링은 인증 분야뿐만 아니라 컴플라이언스 업무에서 고도화해야 하는 영역임을 전달하고자 한다.

ISO37001 도입 및 인증 현황

*제약바이오 업계의 **ISO37001** 도입과 인증은 윤리경영 정착에 긍정적인 신호*

ISO37001은 국제표준화기구(ISO, International Organization for Standardization)에서 공표한 뇌물방지를 위한 경영시스템(Anti-bribery management systems)에 대한 가이드라인과 요구사항이라 할 수 있다.

한국제약바이오협회에서의 2019년 1월 "ISO37001 도입 효과 분석 및 전망" 보고서[2]는 ISO37001이 기업이 뇌물수수 방지를 위해 갖추어야 할 요소들을 구체적으로 명시하여 계획(Plan)→실행(Do)→점검(Check)→개선(Act)의 4단계를 한 사이클로 해 반복적으로 이행함으로써 조직의 부패 리스크를 관리하는 것으로 기술하였다. ISO37001 인증은 조직이 부패방지를 위해 구축한 시스템이 1) ISO 표준에 적합한지 2) 부패방지에 유효한지를 확인하는 것이 목적이며, 특히 최초 인증은 기업이 구축한 시스템이 ISO에서 요구하고 있는 부패방지 기본요건을 만족하고 실질적으로 운영할 준비가 되었는지를 확인하는 데 목적이 있다고 말하고 있다. 협회에서는 ISO37001 도입 및 인증 과정을 통해 업계 내 윤리경영이 기업문화로 정착되어 가는 것으로 평가하고 있다.

1) 약사법 제47조의2 및 의료기기법 제13조의2(경제적 이익 등 제공 내역에 관한 지출보고서 제출 등) 개정에 따라 시행된 내용으로 의약품 공급자가 의료인 등에 제공한 경제적 이익에 관한 내용과 그 근거 자료를 기록하여 보관하고, 필요한 경우 보건복지부 장관에 그 내용을 보고하도록 하는 제도

2) 한국제약바이오협회, ISO37001 도입효과 분석 및 전망, 2019.1

그림 **1. ISO37001** 도입 인증 현황 [2)]

추진일정	참여기업
2017.12 ~ 2018. 5	GC녹십자, 대웅제약, 대원제약, 동아ST, 일동제약, 유한양행, JW중외제약, 한미약품, 코오롱제약
2018. 5 ~ 2018. 10	동구바이오, 명인제약, 안국약품, 종근당, 휴온스, 보령제약,
2018. 10 ~ 2019. 3	엠지, 영진약품

* 17개 제약기업이 최초 인증을 받았음.

ISO37001의 구조

*리스크 평가(**Risk Assessment**)와 모니터링이 필수*

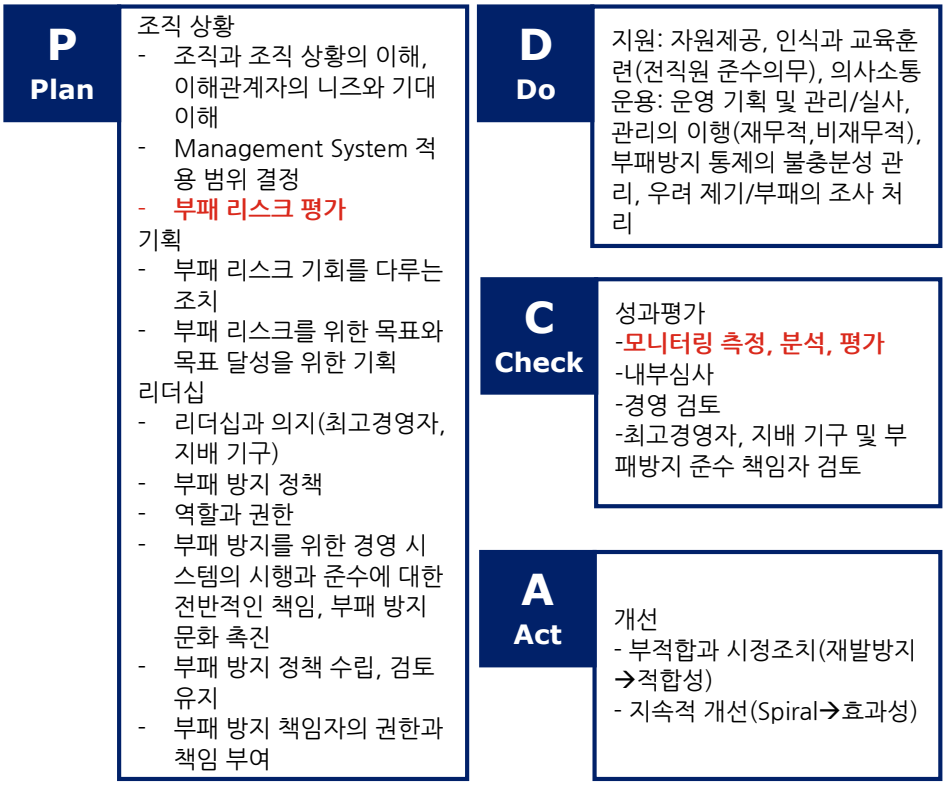
ISO37001은 모든 국가 및 조직에 적용할 수 있는 국제적인 기준을 제시하고 있으며, 특히 부패와 뇌물 위험에 합리적이고, 리스크에 비례하는 방침과 절차 수립, 내부 통제 실행을 위한 요구사항을 명시하고 있다. 표준 요구사항에 적합하다는 인증이 부패와 뇌물 이슈가 없거나 향후 없을 것이라고 보증하지는 못하지만 부패와 뇌물 이슈에 대한 사전 예방, 탐지, 해결하기 위한 합리적이고 리스크에 비례하는 접근방안을 제시하는 것으로 평가받고 있다.

"리스크에 비례한 방침"이라는 것은 리스크 평가(Risk Assessment)가 ISO37001 인증과 운영을 위해 필수불가결한 영역임을 말한다. 리스크 평가 관련하여 주기적인-특정 시기가 정해진 것은 아니나 보통 연 단위-평가를 수행해야 하는 점, 조직별(영업, 마케팅, 임상, R&D, 재무 등)로 리스크 식별이 수행되어야 하는 점, 전사 레벨에서 리스크 영향력 평가 및 우선순위 설정이 필요한 점, 리스크를 완화하기 위한 통제 조치들을 수립하고 운영해야 하는 점 등이 조직 입장에서 준비해야 하는 부분이다.

더불어 수립된 방침과 절차 및 실행에 대한 성과평가를 위하여 모니터링 절차가 필요하다. 모니터링이 필요한 분야와 측정 방안, 모니터링 운영과 책임자 선정, 지속적인 모니터링 고도화(측정 및 분석 결과의 적정성 개선), 모니터링 시점과 결과 보고 라인 결정 등 조직은 문서화된 모니터링 프레임과 결과물 관리가 필요하며, 이를 통해 반부패경영시스템의 효과성과 효율성을 평가받는다.

2) 한국제약바이오협회, ISO37001 도입효과 분석 및 전망, 2019.1

그림 **2. ISO37001 구조** [3)]



디지털 기술의 적용이 가능한 우선순위 영역

앞서 말한 바와 같이 ISO37001에 있어 리스크 평가와 모니터링은 조직 입장에서 준비하고 관리되어야 하는 영역으로 판단된다. 하지만 현재 이 영역에 대해 많은 사람들은 어려움을 겪고 있다. 이는 평가대상이 방대하고 전문지식을 요구하는 영역이기 때문인 것으로 필자는 이해하고 있다.

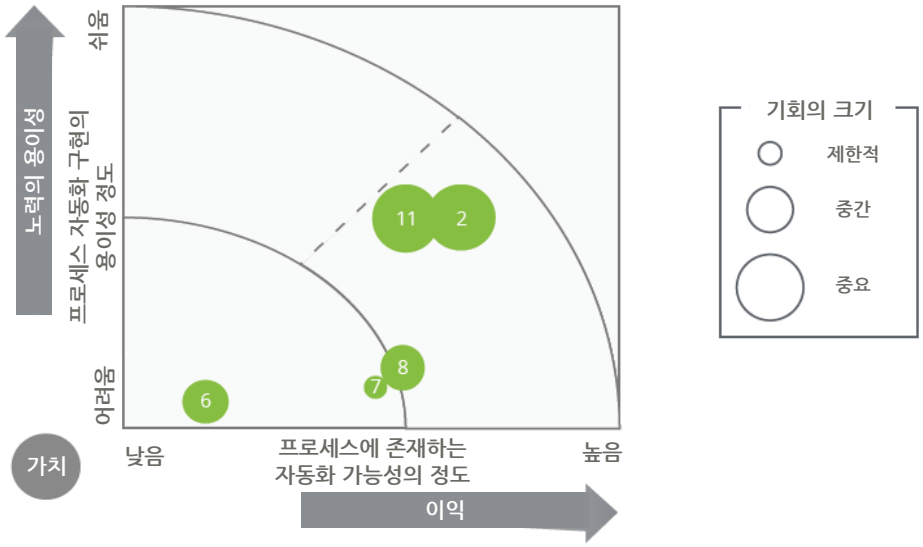
이 상황을 조금 더 유연하게 접근할 수 있는 아이디어는 다음의 보고서에서 찾아볼 수 있다. 딜로이트 보고서, "제약 회사 컴플라이언스에서 가치를 유지하기"에서는 제약회사 컴플라이언스 부서가 해외 부패 및 뇌물 수수, 환자 및 의료 전문가(health care professional)와의 소통, 규제 기관에 대한 보고 등을 포함해 다양한 분야의 업무를 수행함에 있어, 각 분야의 전문지식이 필요하고 다른 부서(영업, 마케팅, 임상 등) 데이터를 검토해야 하기 때문에 전통적으로 수작업 업무가 많다고 말하고 있다.

3) 국민권익위원회, 기업윤리 브리프스, 2018.2.

이때 디지털 기술 적용이 이루어질 경우, 컴플라이언스 부서가 전통적인 수작업 업무에서 벗어나 점점 커져가는 데이터 규모에 뒤처지지 않으면서 무엇이 잘못될 수 있는지 예측하고 예방하는, 가치를 창출하는 조직으로 변환할 수 있을 것이라고 언급하였다. 그리고 디지털 기술 적용을 고려할 때 자동화 가능성, 구현의 용이성, 조직에 대한 가치를 고려하여 아래와 같은 우선 순위 매트릭스로 표현하였으며, 기업의 이익과 투입 시간을 고려할 때 리스크 평가와 모니터링을 우선 순위로 제시하였다.

해당 영역은 ISO37001에서의 주요 부분이자 사람들이 어려움을 겪고 있는 사항과 일치하는 것으로, 국내 제약사에서 보고서가 말하는 디지털 기술의 적용을 어떻게 현실화할 수 있는지 조금 더 살펴보도록 한다.

그림 3. 컴플라이언스에서 자동화 기회를 평가하기 위한 우선 순위 매트릭스 [4]



컴플라이언스 프로세스

1. 거버넌스
2. 리스크 평가
3. 정책 및 절차
4. **M&A** 컴플라이언스 리스크 평가/ 제삼자 공동서류검토회의
5. 교육 및 소통
6. 기밀 보고 및 단계적 확대
7. 조사
8. 시정 및 예방 조치
9. 상부/문화의 어조
10. 지속적인 개선
11. 모니터링

4) Deloitte Insight, "Maintaining value in pharmaceutical compliance" , 2019

리스크 평가, 정보자산에 대한 접근 사례

컴플라이언스 측면에서의 리스크 평가는 인증 보다 더 넓은 범위를 포함

리스크 평가는 기업 내부적인 이슈-배임, 횡령 등-에 의해 새롭게 평가되고 수정되기도 하지만 외부 규제나 시장 상황 변화에 맞게 리스크 평가를 수정해야 하는 경우가 빈번하게 발생한다.

개인정보 보호의 중요성은 날로 강화되고 있으며, 업계에서의 관심도 또한 매우 높아 이러한 경향에 맞춰 새롭게 리스크 평가를 수행하는 경우를 설명하고자 한다. ISO37001은 반부패 경영시스템 중심이기 때문에 개인정보보호를 비롯한 정보자산과 별개로 생각할 수 있다. 하지만 컴플라이언스 부서는 리스크 평가를 단순히 인증만을 위해 운영하는 것보다 윤리경영 정착을 목표로 접근하는 것이 옳은 방향이므로 전사적인 리스크를 고려한 접근이 필요함을 우선 말하고 싶다.

정보 유출로 인한 회사의 피해는 정량적인 수치뿐만 아니라 회사의 평판이라는 정성적인 측면에서도 상당한 위험요인이다. 정보보안은 사고가 발생하기 전에 예방하는 절차가 중요하지만 사고 발생 후에야 사실을 인식하고 사후 대응하기 바쁜 것이 현실이다. 그래서 더욱 사전에 리스크 평가가 진행되어야 한다.

개인정보보호 실태조사의 조사항목[5]은 개인정보수집, 개인정보 이용 및 처리, 영상정보 처리 기기, 개인정보 안전 관리(암호화 대상 암호화 등), 개인정보보호 조직 및 예산, 개인정보보호 교육 등과 관련된 사항이다. 해당 항목에 대한 가이드라인을 확보할 수 있기 때문에 점검 포인트를 내부 운영 현황에 맞춰 리스크를 정의하고, 통제 방안을 수립하는 절차를 진행하는 것이 일반적이다.

개인정보보호 관련 리스크 평가를 진행할 때 회사의 정보 자산 관리도 함께 점검하는 것을 권장하고 있다. 회사 내 프로세스 점검, 법무팀 그리고 IT 부서와의 협업이 필요한 일이므로 개인정보에 국한시키는 것이 아니라 회사 내 정보 자산에 대한 실태조사 방식을 취하면, 한정된 자원으로 효과적인 리스크 평가 진행이 가능하기 때문이다. 개인정보와 함께 검토할 수 있는 정보 자산으로는 제조 관련 기술, 영업 비밀(판매정책, 운영 가이드라인 등), 미공개 정보(R&D, 임상 현황 등)를 활용한 부당이득 취득이 가능한 정보 등이 있다.

정보보안은 정보 자산 식별 및 평가, 정보보호 현황 평가, 국제기준 정보보호체계 진단, 정보보안 전략 수립, 시스템 취약점 진단 및 평가, 정보 유출 가능성 진단, 사후대응 체계 수립, 개인정보보호 강화, 정보 유출에 관한 모니터링 등 많은 전문 서비스 영역이 존재한다. 모든 영역을 한 번에 검토하는 것은 현실적으로 어려운 일이라 기초 자료로 활용될 수 있는 정보자산에 대한 전반적인 리스크 평가를 수행하고, 리스크를 식별하는 과정에서 우선순위 영역을 선정할 수 있다.

5) 행정안전부, 개인정보보호위원회, 2017개인정보보실태조사, "조사내용 및 항목" 중 일부

정보자산은 각종 보안 솔루션들을 통해 보호하는 것이 일반적이기 때문에 디지털 기술에 대한 이해와 접근이 필요하다. 또한, 보안사고를 완전히 막을 수는 없겠으나 사고의 영향력을 최소화하기 위해 정보보안 환경 구축 및 인식의 제고가 필요하다. 이러한 사전 예방은 정보 자산 유출로 인한 재무적 손실 방지, 기업의 이미지 하락 방지, 내부통제 강화 및 임직원의 인식 강화를 목적으로 둔다.

모니터링, 사후 적발에서 사전 예방으로의 변화

수작업 업무 대신 컴플라이언스 본연의 업무에 집중할 수 있도록 하는 것이 디지털 기술의 효과

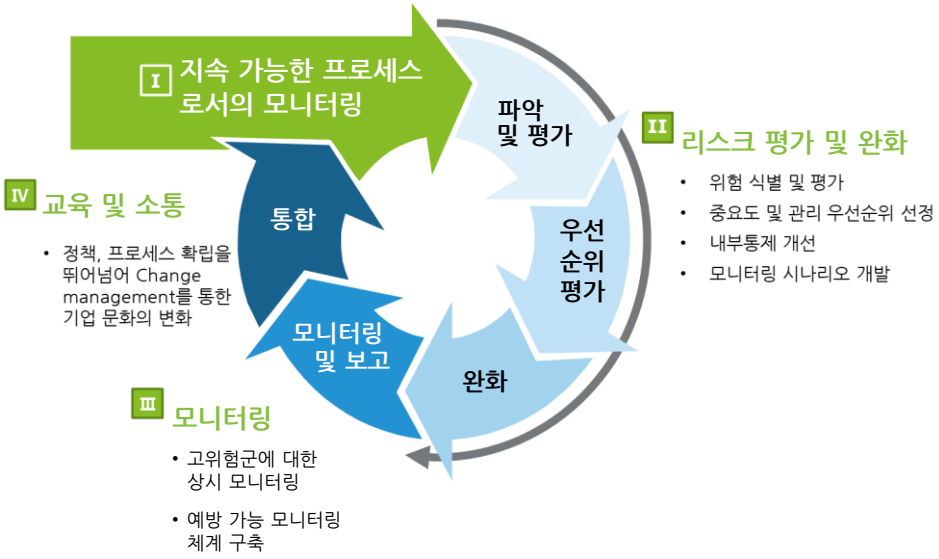
회사의 모니터링은 지속적인 프로세스로 정착되는 것을 목표로 한다. 리스크 평가, 내부 통제안 수립 및 운영, 모니터링 수행, 내부 교육 및 개선 등의 선순환 구조를 지향하는 것이 국제적인 기준이라고 볼 수 있다.

IT 기반의 모니터링 운영을 위해서 리스크 식별에 기반한 시나리오 선정작업이 필요하다. 시나리오 선정은 관련 부서(컴플라이언스, 영업, 마케팅, 재무, 인사, IT 등)에 보관되고 있는 데이터 수집과 데이터 가용성 평가가 수반되어야 한다.

공공기관에서 일반적으로 활용하는 법인카드 모니터링 시나리오는 분할 결제, 주말/휴일 사용, 심야시간 사용, 상품권 구매 등이 있다. 제약업계에서 적용할 수 있는 모니터링 시나리오는 법인카드와 연계하는 경우 제품설명회 식음료비 제공, 퇴근 시간 이후의 법인카드 결제건과 제품설명회와의 연관성 분석 등이 있고, 법인카드 외 독립적인 시나리오로는 견본품 제공, 대금 결제조건에 따른 비용 할인, 재무 측면-도매상 수금, 마케팅 비용 등-과 HR 데이터와의 연계 시나리오를 운영할 수 있다.

모니터링 운영자가 수작업 기반의 시나리오 위반 사항을 검출하는 검토 과정-데이터베이스로부터 데이터를 전자문서 형태로 다운로드받아 샘플링 또는 특정 부서를 타겟으로 한 모니터링 업무-에 긴 시간을 투입하였다면, 시스템 기반 모니터링은 검출된 내역에 대한 직원들의 소명 관리와 기업문화 개선에 더 많은 시간을 투입할 수 있도록 해준다.

그림 4. 모니터링의 선순환 구조



마무리하며

리스크 평가와 모니터링은 컴플라이언스 부서의 핵심과제로 판단된다. 두 가지 영역은 디지털 기술이 적용될 경우 투입 인력을 효율적으로 운영할 수 있게 하며, 컴플라이언스 부서가 지향하는 사전 예방 중심 활동에 온전히 시간을 투입할 수 있도록 할 것이다.

Contact

김성일 부장
FA Financial Crisis
sungilkim@deloitte.com

Deloitte.