GLOBAL PERSPECTIVES & INSIGHTS

글로벌한 관점과 통찰 (GPI)

부정행위 (FRAUD)

파트 1 : 암호화폐와 관련된 부정행위

파트 2 : 내부감사인과 사기심사관 (Fraud Examiner) : 뜻깊은 파트너십

파트 3 : 후유증 : 포스트 코로나 시대의 부정행위

The Institute of Internal Auditors

파트 1

암호화폐와 관련된 부정행위

전문가 소개

데이나 로렌스(Dana Lawrence), CIA, CRMA, CFSA, CAMS, CRVPM

데이나 로렌스는 피디시오(Fideseo)의 최고준법감시인이다. 그녀는 복잡한 컴플라이언스, 전사리스크관리(ERM), 내부감사, 거버넌스 프로그램 수립, 확산 및 해결 분야에서 인정받는 전문가이자 리더이다. 로렌스의 기술 및 금융 서비스 분야 경력은 모기지, 커뮤니티 뱅킹, 미국과 글로벌 대형 은행, 오픈 뱅킹 파트너, 핀테크, 암호화폐를 망라한다. 그녀는 은행 규제기관 및 내부/외부 감사인과 직접 협력하며 고위 리더십 역할을 맡았다. 로렌스는 최대 40,000명이 참석하는 지역, 국가 및 글로벌 행사에서 연설하는 인기있는 대중 연설가이자 이벤트 주최자이다. 그녀는 IIA와 같은 다양한 그룹에 봉사하는 헌신적인 자원 봉사자이자 사고 리더(Thought Leader)이다.

로데스 미란다(Lourdes Miranda), CAMS, CCE, CCFI, CEIC, CFE, CRC, FIS, MS

로데스 미란다는 블록체인 기술 회사인 센드크립토(SendCrypto)의 최고준법감시인이다. 그녀는 전 중앙정보국(CIA) 장교이자 연방수사국(FBI) 분석가로 20년 이상 정부 및 기업과 함께 일했으며 전 세계적으로 금융 범죄 수사와 정보의 수집과 분석을 전문으로 하고 있다. 그녀는 자금세탁업체와 테러자금 조달업자를 표적으로 삼는 광범위한 현장 경험을 쌓아 왔다. 미란다는 2017년부터 핀텍스(FinTechs)에서 암호화폐 수석 조사관, 수석 준법감시인, 리스크 매니저로 근무하며 컴플라이언스, 조사, 암호화폐 및 정보 팀과 교육 프로그램을 구축해 왔다. 그녀는 또한 여러 온라인 강좌의 주제 전문 강사이자 저자이며 기고자이기도 하다. 뿐만 아니라 미란다는 캐나다에 소재한 토론토 컴플라이언스 및 자금세탁방지(AML)기업(TCAE)의 자문 위원회 회원(Advisory Board Member)이다.

번역: 이은주(CIA)
- 삼성전자 내부감사팀 근무
- SC제일은행 내부감사부 근무
- 한국씨티은행 내부감사부 근무
- 2003~한국외국어대학교 통번역대학원 영어과 졸업
- 한-영 통역사, 제조, 금융, IT, 법률 등 다양한 분야의 한-영 통역사 활동

들어가며

암호화폐 및 부정행위에 대한 글로벌 담화

암호화폐 거래소 FTX의 카리스마 넘치는 창업자 **샘 뱅크맨-프리드(Sam Bankman-Fried)**의 자산 가치는 한때 265억 달러로 추정됐다. 암호화폐 시장에서 한때 세 번째로 큰 거래소였던 FTX와 그 리더인 뱅크맨-프리드는 블랙록(BlackRock)과 NFL 선수 톰 브래디(Tom Brady)와 같은 많은 유명 투자자들의 사랑을 받았다. 그러나 그는 현대 역사상 가장 극적인 기업 몰락 사건 중 하나로 거의 하룻밤 사이에 전 재산을 잃었다.

뱅크맨-프리드는 2022년 12월 13일 바하마에서 체포되었다. 공개된 보도에 따르면 그는 송금 사기, 송금 사기 모의, 증권 사기, 증권 사기 모의, 자금 세탁 등 다양한 혐의를 받고 있다.

이처럼 믿기 힘든 몰락의 광경에 세간의 관심이 쏠린 반면, 이 사건은 디지털 자산에 관해 더욱 큰 질문을 제기하기도 했다. 토네이도 캐시(Tornado Cash) 및 비츨라토(Bitzlato) 스캔들과 마찬가지로, FTX의 붕괴와 암호화폐 업계에 미친 영향으로 인해 많은 사람들이 암호화폐 자산의 장기적인 생존가능성에 의문을 품게 되었다. 현재의 상태를 일컬어 미국 증권거래위원회(SEC) 위원장 게리 겐슬러(Gary Gensler)는 '와일드 웨스트(Wild West)'라고 불렀다.

암호화폐 자산과 정보를 유지하는 가장 안전한 방법 중 하나인 블록체인 기술을 기반으로 구현되었음에도 불구하고, 세계에서 가장 유명한 암호화폐 거래소 중 하나의 수장인 저명 인사가 대규모 사기를 저지를 수 있다면 그보다 작은 규모로 업계에서 영업하는 회사에게는 어떤 취약점이 존재할 수 있을까?

암호화폐 자산의 급격한 증가로 인해 리스크 환경은 어떻게 바뀌었으며, 조직과 조직의 내부감사부서는 이러한 변화에 어떻게 성공적으로 대응하고 있는가?

부정행위에 관한 3부작 시리즈인 파트 1에서는 암호화폐 자산 세계의 초기에 볼 수 있는 일반적인 사기 계획을 살펴보며 이러한 질문을 다룰 것이다. 이 주제에 대한 자세한 내용을 알아보기 위해 IIA는 최근에 있었던 웹세미나 "부정행위의 관점: 블록체인, 암호화폐 및 KYC"("Fraud perspectives: Blockchain, Crypto, and KYC") 다시보기를 제공할 예정이며, 본고에 언급된 주제 전문가들과의 실시간 Q&A도 진행된다.

암호화폐의 불확실성

흥미진진하지만 리스크가 존재하는 미래

조직의 관심

블록체인 기술은 그 의미가 방대하고 혁신적이지만 개념상으로는 거의 모든 네트워크 구조에서 공유하고 저장할 수 있는 지속적이며 계속 증가하는 디지털 자산 거래의 로그에 지나지 않는다는 점에서 비교적 이해하기 쉽다. 블록체인 기술이 차별화되는 점은, 새로운 거래가 발생할 때마다 블록을 지속적으로 암호화하는 검증 방법을 사용하여 한층 안전하다는 것이다.

블록체인 기술 회사인 센드크립토의 최고준법감시인 로데스 미란다는 "기술 자체는 매우 복잡하고 분석하는 데 수년간의 훈련과 교육이 필요하지만 나는 그 블록체인 자체가 재무제표라고 생각한다"라고 말했다. "블록체인에는 자산을 보낸 사람, 자산의 보관 위치, 인출 여부, 그 결과인 잔고와 관련된 정보가 담겨 있다."

암호화폐는 어쩌면 중앙은행과 같은 조직의 영향으로부터 자유로운 분산형 오픈소스 통화 시스템을 생성하는 블록체인 기술을 활용한 사례 중 가장 널리 알려진 자산인지도 모른다. 블록체인을 기반으로 하는 암호화폐 자산의 다른 예로 대체불가능 토큰(NFT), 분산 원장 기술(DLT), 게임 토큰 등이 있다.

그러나 산업은 빠르게 학습하고 있기 때문에, 전통적인 방법으로는 사실상 조작이 불가능한 보안 기술을 기반으로 암호화폐 자산이 구축되었다고 해서 이를 채택하는 사람이 리스크로부터 면제된다는 의미는 아니다. FTX의 붕괴가 이를 여러 가지 방식으로 보여준다. 예를 들어, 적절한 기업 지배구조 및 내부통제의 미흡이 조직뿐만 아니라 업계 전체의 환경에 걸쳐 투자자들에게 어떤 피해를 줄 수 있는지를 보여주었다.

이는 IIA 회장 겸 CEO인 앤서니 퍼글리스(Anthony Pugliese)가 최근 미국 의회에 보낸 서한에서 미국에서 운영되는 암호화폐 거래소, 블록체인 기술 회사, NFT 마켓플레이스 및 웹3(Web3) 플랫폼에게 기업 지배구조를 강화하는 새로운 요건을 정립할 것을 요구하며 지적한 내용이었다. 퍼글리스는 "수많은 투자자들이 FTX의 실패에 대한 대가를 치르고 있다"라고 말했다. "규제로부터 자유로운 암호화폐 거래소가 스스로 올바른 행동을 할 것이라 기대할 수 없다는 점은 분명하다. 우리는 보다 강력한 기업 지배구조 표준을 요구하고 이러한 거래소가 고객을 보호하지 못할 때 책임지도록 해야 한다. 나쁜 기업이 실패할 때 그 책임을 투자자에게 넘겨서는 안 된다."

퍼글리스는 FTX의 붕괴와 건실한 내부감사부서의 조치를 통해 시장에 미칠 여파가 완화될 수 있음을 강조했다. "FTX의 붕괴는 강력한 내부감사부서가 없는 조직이란 위험한 불장난을 하고 있으며 최악의 경우 자신과 이해관계자를 완전히 예방가능한 재앙에 빠뜨린다는 사실을 상기시켜 주는 최신 사례이다"라고 그는 말했다.

퍼글리스와 다른 사람들의 이러한 우려는 무시되지 않았다. 2023년 1월 3일, 미국의 연방준비은행, 연방예금보험공사(FDIC), 통화감독청(OCC)은 암호화폐에 대한 최초의 공동 성명(joint statement)을 발표했다. 여기에서 그들은 다음을 포함하여 어떤 형태로든 암호화폐를 운영하는 금융 기관에 적용될 수 있는 다양한 리스크를 강조했다.

- 암호화폐 자산 부문 참여자 간의 부정행위 및 사기 리스크
- 보관, 환매 및 소유권과 관련된 법적 불확실성
- 암호화폐 자산 회사의 부정확하거나 오해의 소지가 있는 표현 및 공시
- 암호화폐 시장의 상당한 변동성. 그 결과에는 암호화폐 회사와 관련된 예탁 흐름에 미치는 잠재적 영향이 포함됨
- 불투명한 대출, 투자, 자금조달, 서비스 및 운영 조건을 포함하여 특정 암호화폐 자산 참가자 간의 상호연결성 때문에 존재하는 암호화폐 자산 부문 내의 전염 리스크
- 성숙도와 견실성이 부족한 암호화폐 자산 부문의 리스크 관리 및 거버넌스 관행
- 개방형, 공개 및/또는 분산형 네트워크나 그와 유사한 시스템과 관련된 리스크의 증가

이러한 모든 리스크는 논의할 가치가 있지만(대부분의 경우 암호화폐에 손대는 비(非) 은행 조직에 적용가능), 본고에서는 암호화폐 참여자에게 자행되는 사기 행위와 현재의 환경에서 발견되는 두드러진 행태로 초점을 제한할 것이다.

부정행위를 저지르기에 좋은 환경

계속 확대되는 리스크 환경

사기꾼에게 주어진 새로운 도구

암호화폐 자산은 투명성과 조작을 방지하는 고급화된 암호화처럼 유리한 특성을 많이 가지고 있지만, 이러한 특성으로 인해 암호화폐 자산(및 배후의 블록체인 기술)은 부정행위를 저지르려는 사람들에게 유용한 수단이 되었다.

실제로, 규제당국과 법 집행기관의 관심을 끌었던 것은 사기꾼이 매력을 느끼는 그러한 특성이었다. 거의 30년 동안 CIA와 FBI에서 금융 범죄를 조사해 온 미란다는 "규제당국이 암호화폐 자산에 관심을 갖는 유일한 이유는 사기꾼들이 운영자금 조달과 자금 세탁에 암호화폐를 사용하기 때문이다"라고 말했다. "블록체인은 조작하기가 매우 어렵지만, 범죄 행위를 조장하는 방식으로 활용될 수 있다."

예를 들어, 한 가지 방법은 블록체인 내에서 허위 신원을 사용하는 것이다. 미란다는 "이것은 암호화폐 세계에서 빈번한 일이다"라고 말했다. "악당은 암시장에서 구한 합법적이고 유효한 신원을 사용하여 지갑을 개설할 때 KYC(고객 확인) 온보딩 프로세스를 통과한다. 이러한 신원은 범죄 경력이 없으며 블랙리스트에 올라 있지도 않고 완전히 깨끗하다. 그런 다음 조사관이 자신의 눈으로 직접 확인할 수 있는 사기 동향이 명백히 드러날 때까지 이 깨끗한 명의를 이용해 자금의 흐름을 거의 드러내지 않으며 돈을 이동시킬 수 있다."

암호화폐 산업은 또한 소비자 편의를 위해 설계되었지만 악용될 수 있는 다양한 허점이 있는 여러 수단을 도입했다. 예를 들어 부정행위 개시자는 법 집행기관의 핑(ping)을 피하기 위해 대포폰과 함께 비트코인 ATM과 같은 암호화폐 거래 허브를 활용할 수 있다.

"내가 뉴욕에 있는데 금융 기관에 있는 돈을 옮겨서 마이애미에 있는 악당들에게 줘야 한다고 가정해 보자. 그들은 돈을 빨리 받고 싶어 한다. 수표도 안 받고, IP 주소 핑 때문에 컴퓨터나 노트북도 쓸 수 없는 상황에서 내가 할 수 있는 일은 뉴욕에 있는 비트코인 ATM에 가서 현금과 대포폰을 사용하는 것이다. 이렇게 하면 자금세탁 방지 절차를 우회하면서 악당들에게 돈을 지불할 수 있다. 이것은 부정행위이다"라고 미란다가 말했다.

돼지 도살

악당들이 활용할 수 있는 또 다른 일반적인 사기 수법은 "돼지 도살"이라는 끔찍한 용어로 알려져 있다. 비즈니스 및 기술 컨설팅 회사인 피데시오의 최고준법감시인 데이나 로렌스는 "이것은 기본적으로 사기꾼이 신뢰를 쌓기 위해 오랜 시간을 투자하여 피해자를 살찌운다는 은유적인 개념이다"라고 말했다. 로렌스에 따르면 사기꾼은 어느 공간에서나 시간을 투자할 수 있지만 주로 소셜 미디어나 문자를 통해 몇 주 또는 몇 달에 걸쳐 공을 들인다. 로렌스는 특히 트위터(Twitter)와 같은 소셜 사이트뿐만 아니라 링크드인(LinkedIn)을 선호하는 플랫폼으로 꼽았다.

이 경우, 사기꾼은 일반적으로 자신이 암호화폐 투자에 성공한 인플루언서나 내부자라고 소개한다. 시간이 지나고 피해자가 자신에게 돈을 이체하도록 유도하기 위해 이들은 암호화폐의 이점을 홍보할 것이다. 어떤 경우에는 사기꾼이 피해자에게 위조된 재무제표를 제공하여 상당한 수익을 올리고 있는 것처럼 보이게 만들기도 했다.

이러한 징후는 쉽게 알아차릴 수 있는 반면, 사기꾼의 수법은 한층 교묘해졌다. 예를 들어, 캄보디아와 중국과 같은 국가에 기반을 둔 사기꾼 일당은 사람들이 불합리한 결정을 내리도록 심리적으로 취약하게 만드는 방법에 대해 심리학자들로부터 집중적인 훈련을 받았다. "그들은 사람들을 조종하는 최선의 방법을 찾으려고 심리학자들로부터 훈련을 받았다"라고 캘리포니아주 산타클라라 카운티 지방 검사인 제프 로젠(Jeff Rosen)이 CNN과의 인터뷰(interview)에서 말했다. "당신은 사람을 취약하게 만들고 돈과 떨어지도록 만들기 위해 다양한 심리적 기법을 사용하는 이들을 상대하고 있는 것이다."[1]

펌프앤덤프(Pump and dump)

암호화폐에서 볼 수 있는 또 다른 주요 사기 행태는 주식 시장의 오랜 관찰자들에게 잘 알려져 있는 소위 "펌프앤덤프"(시세조종) 사기이다.

로렌스는 "이 사기는 일반적으로 그룹이 모여 토큰과 같은 새로운 암호화폐 프로젝트를 시작한 다음, 보통 인플루언서의 도움을 받아 리소스를 사용하여 트위터나 디스코드(Discord)와 같은 플랫폼에서 홍보하는 것으로 시작된다"라고 말했다.
"현재 암호화폐 시장에는 유동성으로 인해 많은 변동이 일어난다. 그래서 많은 사람이 한꺼번에 사려고 하면 시장이 일종의 충격을 받아 가격이 오르게 된다. 가격이 상승하면 자산을 대량으로 보유하고 있는 악당은 이익 실현을 위해 자산을 갑자기 매각하고 가격이 급락하면서 다른 투자자들에게는 본질적으로 가치가 0인 자산이 남게 된다."
로렌스는 이러한 상황에서는 모든 것을 잃을 가능성이 있다는 점을 잠재적 투자자에게 알리는 공시가 명백히 부재한다는 점이 위험 신호라고 말했다. 사기꾼은 또한 일반적으로 비슷한 닉네임을 가진 작성자들이 쓴 토론 게시판의 글과 소셜 미디어에 복사하여 붙여넣은 메시지를 적극적으로 활용한다. 그리고 사기행각이 종료되면 이러한 닉네임은 대개 사라지고 익명성은 완전히 지켜진다.

암호화폐 자산에서 발견되는 또다른 사기 사례

암호화폐 기반 사기가 항상 그렇게 정교할 필요는 없다. 암호화폐 기반 조직에서 악당에게 필요한 것은 기회뿐인 경우도 많다. 예를 들어, 블록체인 자체는 디지털 자산을 안전하게 유지하지만 개인 키만 있으면 보안을 우회하여 암호화폐 지갑을 털 수 있다. 개인 키는 레스토랑 냅킨에도 적을 수 있고 누구나 볼 수 있게 아무데나 둘 수 있는 긴 숫자의 연속일 뿐이다.
"당신의 개인 키는 암호화폐 시장에서 디지털 신원이며, 이를 보유한 사람은 누구나 사기 거래를 수행하거나 암호화폐 코인을 훔칠 수 있다"라고 로렌스는 말했다. "만약 누군가가 용케 액세스해서 내 비트코인을 모두 탈취하면, 내가 할 수 있는 일은 아무것도 없다. 돌려받을 수도 없고 민원을 제기할 수도 없으며 이에 대해 이의를 제기할 소비자 보호기관이나 규제기관도 없다. 문자 그대로 사라지는 것이다."
암호화폐 시장의 성숙에 따라 개인 키 및 회사 키를 분실로부터 보호하는 특화된 암호화폐 보안 서비스가 등장했지만 어떤 경우 그 방법론은 놀라울 정도로 원시적이다. 로렌스에 따르면 이러한 서비스 중 일부가 사용하는 솔루션은 황량한 산에 있는 금고에 키를 보관하는 것이다. 암호화폐 보험은 비용을 부담할 수 있는 기업에게 안전망으로 존재하지만 현 단계에서는 업계 전체가 수익성에 어려움을 겪고 있어 보험사들은 고객 선정에 있어 지극히 신중해야 하는데 반면 보장 범위는 해마다 줄어들고 있다.
영국 인슈어런스 타임즈(Insurance Times)에 게재된 기사(article)에서 RPC 보험 그룹 파트너인 제임스 윅스(James Wickes)는 암호화폐 보험 시장의 도전과제에 대해 논의했다. 그는 "현재 암호화폐 자산 보험 분야에서 활동하고 있는 상대적으로 소수의 보험사들은 최근의 폭락에서 알 수 있듯이 암호화폐 시장의 변동성으로 인한 잠재적 노출을 제한하기 위해 보험 약관의 세부 사항을 검토하는 데 열심일 것"이라고 말했다. "암호화폐 자산 보험 시장은 아직 초기 단계이며 보험사들이 수요를 충족할 수 있는 충분한 역량을 제공할 준비가 되어 있는지, 시장이 전통적인 절도 리스크를 넘어 보험 적용 범위를 얼마나 과감하게 확장할 것인지 지켜봐야 한다."[2]
그러나 이러한 예방 조치에도 불구하고 사기꾼이 직접 기존 계정을 우회하지 않고도 암호화폐 자산과 블록체인을 계속 활용하기 위해 사용할 수 있는 특정 도구, 즉 텀블러라고도 알려진 믹서가 남아 있다. 블록체인의 핵심적인 특징 중 하나는 투명성이다. 블록체인 탐색기 내에서는 누구나 2009년 암호화폐가 출시된 이후 발생한 모든 블록체인 거래 기록을 볼 수 있다.
믹서를 사용하면 사용자는 문제의 암호화폐 자산을 의도한 수신자에게 전송하기 전에 암호화폐 자산을 본질적으로 섞을 수 있으며, 누가 누구에게 얼마나 많은 자산을 보냈는지 정확히 해독하기가 어렵기 때문에 어느 정도 익명성을 확보할 수 있다. 믹서를 사용하면 탐색기로 볼 수 있는 정보는 한 사람 또는 수십 명의 다른 이가 자산을 믹서로 보낸 다음 다양한 금액으로 쪼갠 자산을 여러 사람에게 보냈다는 것뿐이다. 그 결과는 본질적으로 완벽한 자금 세탁과 유사하다.
이러한 현실에 직면하여 암호화폐 세계에 남아있기로 선택한 조직은 현 단계에서 리스크 경감과 관련하여 대부분 스스로 책임을 져야 한다는 점을 받아들여야 한다. 이는 암호화폐를 피해야 한다는 의미는 아니지만 컴플라이언스, 건전한 내부통제, 부정행위 탐지 및 억지 노력, 그리고 내부감사가 이사회 수준부터 시작해서 조직 내에서 이루어지는 암호화폐 관련 담화에서 큰 역할을 해야 함을 의미한다.

---

1 Josh Campbell, "Beware the 'Pig Butchering' Crypto Scam Sweeping Across America," December 26, 2022, https://www.cnn.com/2022/12/26/investing/crypto-scams-fbi-tips/index.html.
2 Isobel Rafferty, "Cryptocurrency Crisis Leading to Insurance Policy Wording Amendments," Insurance Times, July 18, 2022, https://www.insurancetimes.co.uk/news/cryptocurrency-crisis-leading-to-insurance-policy-wording-amendments/1441786.article.

내부감사의 출발점

규제의 시작과 더 많은 규제의 등장

지침의 발행

앞서 언급한 바와 같이 기업이 암호화폐 자산 및 관련 부정행위 리스크에 대해 보안과 거버넌스를 위해 고려할 수 있는 규제 프레임워크는 거의 없다. 그러나 금융 서비스와 같은 특정 산업에 디지털 자산 보호에 관한 적절한 거버넌스 원칙을 다루는 리소스가 전혀 없는 것은 아니다. 이 중 다수는 암호화폐에 적용된다.
2022년 10월, 유럽 연합은 암호화폐 마케팅에 대한 포괄적인 규제를 위해 전 세계적으로 최초의 시도 중 하나인 암호자산시장법률(The Markets in Crypto-Assets (MiCA) Regulation) 합의문을 도입했다. 이 법안은 24개 언어로 번역되어야 하기 때문에 2023년 4월까지는 상정 상태이다. 이 법안이 공식 채택되면,

- 공식적으로 암호화폐 자산을 "분산 원장 기술 또는 유사한 기술을 사용하여 전자적으로 전송 및 저장할 수 있는 가치 또는 권리의 디지털 표현"으로 정의한다. 또한 자산준거토큰(asset-referenced tokens), 전자화폐토큰(e-money tokens), 유틸리티 토큰(utility tokens), 그리고 이 세 가지 범주에 속하지 않는 네 번째 범주라는 네 가지 암호화폐 자산 범주를 제공한다.
- 투자자의 암호화폐 자산을 잃을 경우 암호화폐 제공업체에 공식적으로 책임을 지게 한다.
- 암호화폐 자산 시장의 행위자는 환경 및 기후 발자국(Climate Footprint)에 대한 정보를 보고해야 한다.
- 자금세탁 방지에 관한 개정법안과 중복되며, 규정을 준수하지 않는 암호화폐 서비스 제공업체의 공개 등록 관리를 유럽은행감독청(EBA)에 맡길 것이다.
- 암호화폐 자산 제공업체가 EU에서 영업하려면 허가를 받도록 요구한다.
- "스테이블코인"(외부 참조 자산에 고정된 암호화폐)에 적용할 수 있는 강력한 프레임워크를 제공한다. 발행자는 모든 스테이블코인 보유자에게 언제든 이 프레임워크를 통해 청구할 수 있는 권리를 무상으로 제공해야 한다.[3]

미국에서는 연방준비은행, 연방예금보험공사, 통화감독청이 공동으로 발표한 공동 성명(joint statement)이 미국 기업을 위한 몇 가지 리소스를 제공하는데 이 리소스는 "제안되었거나 이미 존재하는 암호화폐 자산 관련 활동에 대해 금융 기관이 강력한 감독 논의에 참여"하는 데 도움이 되도록 고안된 지침을 제공한다."[4]
그러한 지침은 다음과 같다.

- OCC 해석서 1179(OCC Interpretive Letter 1179) "다음을 명시한 수석 고문(Chief Counsel)의 해석: (1) 특정 암호화폐 활동에 참여하는 은행의 권한 (2) 내셔널 트러스트 은행을 설립하는 OCC의 권한."
- 연방준비은행 SR 22-6/ CA 22-6: "연방준비은행이 감독하는 금융 기관의 암호화폐 자산 관련 활동 참여."
- FDIC FIL-16-2022 "암호화폐 관련 활동에 참여하는 FDIC 감독 기관에 대한 통지 및 감독 피드백 절차."

활용가능한 리소스가 이것만 있는 것은 아니다. FTX의 붕괴 이후 SEC도 기업들에게 디지털 상품 회사와의 관계를 공시하도록 권고하는 지침을 발표했다.

---

3 General Secretariat of the Council, "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)," Council of the European Union, October 5, 2022, https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf.

4 "Joint Statement on Crypto-Asset Risks to Banking Organizations, Board of Governors of the Federal Reserve System Federal Deposit Insurance Corporation Office of the Comptroller of the Currency, January 3, 2023, https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf.

교육의 가치

채택 시 상기 EU 법안은 2024년에 발효될 것이지만 이것이 마지막 법안은 아닐 것이다. 규제 환경이 매달 조금씩 완성됨에 따라 내부감사인이 취할 수 있는 가장 중요한 조치는 변경사항을 파악하고 이러한 변경을 이사회와 해당 이해관계자에게 명확하게 설명하기 위해 모든 노력을 기울이는 것이다.

현재 환경에서 내부감사인은 암호화폐 노력에 적용될 수 있는 다른 규정이 무엇인지 이해관계자에게 설명해야 한다. 예를 들어, 자체 암호화폐를 제공하려는 회사는 미국 금융 범죄 집행 네트워크(U.S. Financial Crimes Enforcement Network)에 등록해야 할 수도 있다고 로렌스는 말했다. 이는 암호화폐가 법안에 구체적으로 언급되지 않았기 때문에 쉽게 간과될 수 있는 중요한 세부 사항이다. 그녀는 "지금은 불확실성이 많다"고 말했다. "해당되는 것과 그렇지 않은 것을 리더에게 알리는 것은 내부감사인의 몫이다."

또한 새로운 기술에 초점을 맞추더라도 가상사설망(VPN) 사용, 사용자(특히 소비자) 프로필 정보의 적절한 보안, 수집 및 필요 시 폐기를 포함하여 디지털 자산 보호와 관련된 기본적인 모범 사례를 기업이 간과해서는 안 된다. 미란다는 "사용자 프로필은 조직의 중요한 통제 수단이다"라고 말했다. "내가 회사를 감사한다면 사용자 프로필이 거래 활동과 일치하는지 확인할 것이다. 예를 들어, 지리적 정보는 컴플라이언스 및 조사에 매우 중요하다. 조직은 이 정보를 안전하게 유지하고 정보가 어디에 있는지 알아야 한다." 이 점에서 미란다는 조직이 부정행위 조사 시 중요할 수 있는 물리적 주소처럼 핵심 프로필 정보가 포함된 비밀유지계약(NDA)을 간과하는 경우가 많다는 점을 지적했다.

자세한 내용은 IIA의 추가 지침 "내부감사와 부정행위: 부정행위 리스크 거버넌스의 평가"("Internal Audit and Fraud: Assessing Fraud Risk Governance")에서 부정행위 리스크의 건실한 거버넌스 및 관리를 위한 조직의 역할과 책임에 관한 명확한 지침과, COSO의 부정행위 리스크 관리 가이드 (Fraud Risk Management Guide)와 같은 추가 지침 권고사항을 제공하고 있다.

마치며

내부감사의 준비

암호화폐와 그 기반 기술은 내부감사가 무시하기에는 너무나 혁신적이며, 이사회의 관심 이상으로 중요하다. 이를 무시하는 리스크 평가에는 치명적인 맹점이 있다. 암호화폐는 많은 사람들에게 상대적으로 새로운 개념일 수 있지만 그렇다고 내부감사가 부정행위 리스크를 측정하고 테스트할 수 있는 건실한 관리 프레임워크의 중요성을 감소시키지 않는다.

이미 확대되고 있는 내부감사의 레이더에 추가할 또 다른 리스크 영역이 생겼다고 한탄하기 쉽지만, 이를 해결하는데 내부 감사보다 더 나은 위치에 있는 조직내 부서는 없다는 것은 좋은 소식이다. 2002년 SOX법(Sarbanes-Oxley Act)이 그랬던 것처럼, 암호화폐 규제의 진화는 사실상 내부감사가 앞으로 수년간 테이블에서 중요한 위치를 차지할 수 있도록 보장한다. 아직 암호화폐에 대해 잘 알지 못하더라도 내부감사부서는 부정행위가 무엇인지에 대해서는 알고 있으며 리스크에 대해서도 잘 알고 있다. 그것만으로도 내부감사를 준비시켜 앞으로의 과제를 해결하는 리더십 위치를 차지하기에 충분하다.

파트 2

내부감사인과 사기심사관(Fraud Examiner): 뜻깊은 파트너십

전문가 소개

메이슨 윌더(Mason Wilder), CFE

메이슨 윌더는 공인사기심사관(CFE)이자 공인사기심사관협회(ACFE)의 연구 매니저이다. 그는 보수교육(CPE)을 위한 ACFE 자료의 작성과 업데이트를 감독하고 모든 ACFE 교육 행사의 기획과 제작을 지원하며 국가 보고서(Report to the Nations) 및 벤치마킹 보고서와 같은 연구 이니셔티브에 참여하고, 교육을 실시하고, ACFE 간행물에 기고하고, 회원과 언론의 요청에 대응한다. ACFE에 합류하기 전에 윌더는 10년 넘게 기업 보안 인텔리전스 및 조사 분야에서 일했으며 국제적인 물리적 보안과 위기 대응을 위한 신원 조회, 실사, 인텔리전스 분석을 전문으로 했다. 메이슨은 주요 의사 결정을 지원하기 위해 모든 소스에서 관련 정보를 수집, 분석, 정제하는 데 경력을 쌓았으며 부정행위 방지 전문가가 부정행위에 효과적으로 대항할 수 있는 능력을 지속적으로 향상시키는 데 열정을 쏟고 있다.

셔나 플랜더스(Shawna Flanders), CRISC, CISA, CISM, SSGB, SSBB

IIA의 프로덕트 개발 이사인 셔나 플랜더스는 기술적인 대화를 일반적인 비즈니스 언어로 변환하려는 열정을 지닌 기술인이자 기술 교육 업계 전문가이다. 셔나는 SME 콘텐츠 개발/기여, 연설/교육, IT 관련 리스크, IT 감사, 정보/사이버보안, IT 컴플라이언스, IT 거버넌스, 공급업체 관리, 통신분야 IT 총괄, 프로그래밍, 음성/데이터 관련 아키텍처 설계/검토, 엔지니어링, 애널리틱스/통합 관리, 비즈니스 프로세스 관리, 비즈니스 분석, 프로젝트 관리, 프로그램 관리 및 프로세스 개선/식스 시그마를 포함하여 모든 감사업무에 고유하고 상보적인 스킬의 조합을 제공한다.

번역: 이은주(CIA)
- 삼성전자 내부감사팀 근무
- SC제일은행 내부감사부 근무
- 한국씨티은행 내부감사부 근무
- 2003~한국외국어대학교 통번역대학원 영어과 졸업
- 한-영 통역사, 제조, 금융, IT, 법률 등 다양한 분야의 한-영 통역사 활동

들어가며

내부감사인은 부정행위의 식별 및 경감을 포함하여 조직이 리스크를 관리하는 데 도움이 되는 거버넌스, 리스크, 내부통제에 대한 **건설적인 통찰력을 제공한다**. 부정행위의 탐지 및 억지에서 내부감사가 효과적인 부분이긴 하지만 부정행위를 적발하는 것은 내부감사인의 업무가 아니다. 반면 공인사기심사관의 특화된 임무는 부정행위를 식별하고 조사하는 것이다. CFE는 부정행위와의 전쟁에서 전문적인 스킬을 제공한다. 결과적으로 두 유형의 전문가가 조직의 최선의 이익에 부합하는 파트너십을 통해 협력하는 것이 합리적이다.
부정행위에 관한 3부작 시리즈 중 두 번째인 본고에서는 내부감사인과 CFE 간의 공생 관계를 구축함으로써 얻을 수 있는 이점을 검토한다.

부정행위의 범위

부정행위로 인해 발생하는 평균 손실액: 약 180만 달러

만연한 리스크로 남아있는 부정행위

부정행위는 금전적 또는 개인적 이득을 위해 수행되는 기망, 은폐 또는 배임과 관련된 **모든 불법 행위이다**. 부정행위를 저지르는 사람이나 조직은 돈, 재산 또는 서비스를 훔치거나, 대가를 치르거나 무언가를 잃지 않기 위해, 개인적 또는 사업적 이익을 취하기 위해 이를 저지를 수 있다. 외부의 사기꾼 외에도 재정적 곤란을 겪고 있거나 조직이 자신을 부당하게 대우했다고 생각하거나 다른 불만을 품고 조직이 자신에게 돈이나 서비스를 빚졌다고 생각하는 내부 직원이 부정행위를 저지를 수 있다. 모든 조직은 유형과 규모에 무관하게 공공 부문이건 민간 부문이건, 비영리, 정부 기관, 공기업 또는 사기업, 기타 법인 여부에 관계없이 부정행위의 피해자가 될 수 있다.

부정행위는 조직에 심각하고 만연한 리스크이다. 부정행위의 결과는 업무 마비에서부터 조직의 존폐를 위협하는 데 이르기까지 다양하다. 재정적 어려움과 손실뿐만 아니라 운영, 수익 또는 이익에 피해를 주는 비효율성, 프로젝트의 취소, 그리고 범위에 따라서는 조직의 패망도 포함될 수 있다.[5]

ACFE가 전 세계 CFE를 대상으로 실시한 조사에서는 133개국에서 발생한 2,110건의 부정행위 사례를 다루었다. 해당 조사에서 부정행위로 인한 전 세계 손실은 총 36억 달러가 넘었으며 건당 평균 손실액은 거의 180만 달러에 달했다. 실제로 CFE는 조직이 매년 부정행위로 인해 수익의 5%를 잃는다고 추정한다. 분명히 부정행위 리스크는 중소기업에서 가장 높다. 직원 수가 가장 적은 회사에서 손실액 중앙값이 가장 높았다(15만 달러).

이 정도 규모의 손실은 쉽게 적발할 수 있지만, 부정행위는 작은 규모로 시작됐다가 시간의 흐름과 함께 누적되어 발생하는 경우가 많다. 해당 설문조사에 따르면 통상적인 부정행위로 인해 한 달에 8,300달러의 손실이 발생할 수 있으며 적발하는 데 12개월이 걸릴 수 있다. 일부 부정행위에 암호화폐가 연루되어 있다는 사실을 아는 것도 중요하다. ACFE는 암호화폐가 8%의 사건에 관여한 것으로 밝혀냈다. 일반적인 시나리오에는 뇌물 수수, 리베이트 제공, 자산의 유용 및 전환이 포함된다.[6]

직장내 부정행위의 카테고리

ACFE 2022 국가 보고서에 따르면 직장내 부정행위에는 3대 카테고리가 있다.

재무제표 분식 사기나 조직의 재무제표에 중대한 왜곡 또는 누락을 초래하는 행위는 가장 흔하지 않았지만(9%) 가장 손실이 컸으며 건당 손실액은 593,000달러였다.

직원이 회사 자원을 훔치거나 남용하는 **자산 유용**은 86%에서 발생했다. 그러나 평균 손실액은 건당 100,000달러로 가장 낮았다.

뇌물 수수, 이해 상충, 강탈 등을 포함한 **부패**가 사건의 50%에 관련되어 건당 150,000달러의 손실을 입혔다.

출처: *Occupational Fraud 2022: A Report to the Nations*, Association of Certified Fraud Examiners.

5 IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.

6 *Occupational Fraud 2022: A Report to the Nations*, the Association of Certified Fraud Examiners.

내부감사인의 역할

부정행위 예방에 대한 검증/조언

내부감사의 중심인 부정행위 탐지/억지

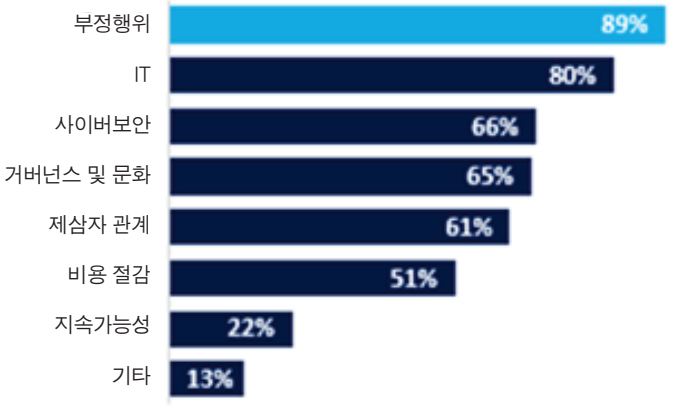
IIA에 따르면, "내부감사직무는 조직의 운영을 개선하고 가치를 더하기 위해 고안된 독립적이고 객관적인 검증 및 컨설팅 활동이다. 그 역할에는 부정행위 리스크를 탐지, 예방, 모니터링하고 감사 및 조사에서 이러한 리스크를 다루는 것이 포함된다."[7]

조직은 내부감사의 스킬에 부정행위 조사가 포함될 것이라 기대해서는 안 된다. 상황에 따라 내부감사가 조사 역할을 수행해야 하는 경우 내부감사인은 신중한 주의를 기울여야 하며 필요한 경험과 전문성이 없는 경우 조사를 진행해서는 안 된다.

부정행위 예방은 경영진의 역할이지만, 내부감사는 부정행위를 탐지하고 억지하기 위해 고안된 내부통제에 대해 필요한 검증 서비스를 제공함으로써 부정행위 방지 관리 노력을 돕는다. 부정행위는 통제 설계의 미비점과 거버넌스의 취약점으로 인해 조직의 프로세스를 훼손하는 경우가 많다. ACFE 설문조사 사례 중 거의 절반이 내부통제 부족(29%) 또는 기존 통제의 무효화(20%)로 인해 발생했다. 감사인은 조사 영역에서 부정행위 리스크의 가능성과 내부통제의 적절성을 고려한다. 설문조사에 따르면 부정행위 방지 통제가 마련되면 부정행위 손실이 줄어들고 부정행위가 보다 신속하게 탐지되는 경향이 있다.

부정행위 방지 노력에 대한 내부감사의 기여를 과소평가해서는 안 된다. IIA가 최고감사책임자(CAE)들에게 내부감사부서가 유의미하게 관여한 부분을 물었을 때 57%는 부정행위, 56%는 전반적인 리스크 평가를 꼽았다.[8] 한편, ACFE 조사에 따르면 내부감사부서가 존재하지 않을 때 부정행위 손실의 중앙값은 50% 더 높은 것으로 나타났다(150,000 달러 대 100,000 달러).

감사에 통합되어 있는 고려사항



출처: 2023 North American Pulse of Internal Audit report

IIA의 북미 내부감사의 맥박 설문조사, 2022년 10월 20일부터 12월 2일까지. Q25: 일반적으로 감사업무를 수행할 때 다음 중 일반적으로 고려하는 영역은 무엇인가? (해당되는 항목은 모두 선택) n = 555.

7 IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019.

8 2022 Premier Global Research, *Internal Audit: A Global View*, Internal Audit Foundation, 2022.

실제로, 다가오는 2023년 북미 내부감사의 맥박(North American Pulse of Internal Audit) 보고서의 데이터에 따르면 부정행위는 내부감사에서 가장 자주 언급되는 고려사항이다. 북미 최고감사책임자들을 대상으로 한 이 연례 설문조사에서는 500명 이상의 응답자에게 일반적인 감사의 일부로 어떤 영역을 포함하는지 질문했다. 2023년 3월 GAM 컨퍼런스에서 공개된 보고서에 따르면 "응답자들은 감사인이 종종 총체적인 접근방식을 취하고 사이버보안, 제3자, 거버넌스를 포함한 광범위한 문제를 고려한다"고 한다. 전체적으로 CAE의 89%는 일반적으로 모든 감사에 부정행위를 고려한다고 답했다. 부정행위는 가장 자주 언급된 리스크 범주로, 2위는 80%를 차지한 IT였다.

부정행위 및 내부감사에 관한 IIA 입장서: 성공을 위한 부정행위 통제의 기본 검증[9] (*IIA Position Paper on Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*)에 따르면, 내부감사인은 다음을 수행할 수 있도록 부정행위에 대해 필요한 지식을 갖추어야 한다.

- 부정행위의 발생을 가리킬 수 있는 위험 신호를 식별
- 부정행위의 특성과 부정행위에 사용되는 수법, 부정행위의 계획 및 시나리오 유형을 이해
- 추가 조치가 필요한지 또는 조사를 권고해야 하는지 결정할 수 있는 능력
- 부정행위를 예방 또는 탐지하고 개선 기회를 식별하기 위해 통제 효율성을 평가

9 IIA Position Paper, *Fraud and Internal Audit: Assurance over Fraud Controls Fundamental to Success*, IIA, 2019

사기 심사관의 역할

기망행위의 조사

숙련된 부정행위 조사의 중요성

사기 심사관은 조직의 전반적인 부정행위 심사 프로그램에 **참여하고 지원을 제공한다.** 그들은 "무슨 일이 일어났는지 확인하고, 책임있는 당사자를 식별하고, 해당되는 경우 권고사항을 제공하는 데 도움이 되는 사실과 증거를 얻으려고 노력하는" 부정행위 조사를 수행함으로써 이를 부분적으로 수행한다.[10] 심사관이 조사를 시작할 때 고려하는 이슈 중 하나는 예측이다. 이는 잘 훈련된 전문가의 눈에 부정행위가 발생했음이 타당해 보이는 상황의 전체성이 있어야 함을 의미한다.

사기 심사관의 조사 단계에는 증거 확보, 발견 내용 보고, 필요 시 보고 내용에 대한 증언, 부정행위 탐지 및 예방 지원 등이 포함될 수 있다. 일반적으로 부정행위 심사의 두 가지 목적은 잠재적인 부정행위 또는 부정행위 혐의에 대한 조사와 조직의 부정행위방지 정책 및 통제에 대한 검토이다. 부정행위 심사의 보다 구체적인 목표는 다음과 같다.

- 부정행위와 연루되어 있거나 연루될 수 있는 부적절한 행동을 찾아내고 그러한 행동의 책임 소재를 판단
- 부정행위로 인한 실제 발생하였거나 잠재적인 손실 또는 책임을 판단
- 부정행위를 식별하고 경감하려는 조직의 의지 표현
- 손실 복구 촉진을 도움
- 향후 부정행위 및 관련 손실이나 책임을 예방
- 금전적 손실 외의 결과를 해결
- 내부통제의 취약점을 찾아 강화
- 경우에 따라 필요 시 법령, 규정, 계약 또는 관습법 의무를 준수[11]

10 *"Planning and Conducting a Fraud Examination,"* Fraud Examiners Manual: 2022 Edition, ACFE.

11 ibid

접근법의 비교

다음의 표는 내부감사인과 CFE의 역할, 접근법 및 목표 간의 몇 가지 중요한 차이점에 대한 개요이다.

특성	내부감사	부정행위 심사
의도	내부감사 절차를 통해 부정행위를 적발할 수 있지만 적발이 보장되는 것은 아니다. 예를 들어, 감사인은 검토 과정에서 의심스러운 거래나 상황을 발견하고 궁극적으로 부정행위로 식별할 수 있다. 그러나 부정행위의 적발은 감사 대상 영역 내 통제 및 절차에 대한 대규모 심사의 한 측면일 뿐이다.	부정행위 심사는 부정행위를 발견하고 부정행위방지 조치 또는 활동을 고려하는 데 직접적으로 초점을 맞춘다.
실시	감사는 대개 정기적으로 실시되며, 한 영역의 고유한 상황이나 의문을 다루기 위해 특별 감사가 실시될 수 있다.	부정행위 조사는 리스크 관리 또는 부정행위 리스크 평가 프로그램의 일환으로 특정 트리거 없이 실시될 수 있지만 일반적으로 충분한 예측이 있는 경우에만 수행된다. 대부분은 제보에 의해서나 혐의에 대한 대응으로 수행된다. ACFE 설문조사에 따르면 부정행위의 43%가 제보로 인해 적발되었으며, 이는 그 다음으로 일반적인 방법보다 거의 3배나 높은 부정행위 적발 방법이었다. 전체 부정행위 제보 중 절반 이상이 직원에게서 나왔다.
적대성 여부	내부감사는 본질적으로 비적대적이다. 예를 들어 감사인의 목표는 팀장과 팀원이 통제나 기타 프로세스를 개선하는 데 활용할 수 있는 통찰력과 정보를 제공하는 것이다.	부정행위 심사는 본질적으로 적대적이다. 목표의 일부는 부정행위를 저지른 사람을 처벌하는 것이다.
기준	내부감사인은 IIA가 정한 국제내부감사표준(*International Standards for the Professional Practice of Internal Auditing*)을 따른다.	CFE는 ACFE 전문 표준 강령(*Code of Professional Standards*)을 따른다. CFE는 심사 중 ACFE 부정행위 리스크 평가 도구(*fraud risk assessment tool*)를 사용할 수 있다.

협업의 활용

상호 존중과 책임

부정행위와의 전쟁

감사인과 사기 심사관 사이에는 상호 **유리하게 협력할 수 있는 많은 기회가 있다**. 그들은 다음 사항에 관해 서로 협의할 수 있다.

- 부정행위 조사 착수
- 감사 및 사기 심사의 연례 기획
- 리스크 평가
- 통제 및 부정행위방지 프로그램의 평가
- 부정행위를 암시하는 감사 지적사항의 전달
- 통제 미비점의 해결

많은 조직에는 내부감사가 발견한 부정행위 의혹을 외부 또는 내부의 사기 심사팀에 전달할 때 프로토콜을 관리하는 규칙이 있다. 내부감사팀은 부정행위 발견사항을 기록하고 검토가 끝나면 사기 심사관과 공동 보고서를 작성한다.
또한 내부감사에서는 조직의 부정행위방지 부서를 감사하여 자체적인 통제가 적절한지 확인할 수 있다. 부정행위방지 팀은 여러 영역 중에서 내부감사를 포함하여 법률 또는 전사리스크관리 팀에 보고할 수 있다. 부정행위방지 팀이 내부감사에 보고하는 경우 부정행위방지 부서의 감사는 객관성을 보장하기 위해 아웃소싱되어야 한다.

직장에서의 협업 사례

다음 사례 연구는 두 팀이 어떻게 협력할 수 있는지 보여준다. 이는 최근 IIA 및 ACFE의 웹세미나 "협력의 촉진: 감사인과 사기 심사관(Fostering Collaboration: The Auditor and the Fraud Examiner)"에서 있었던 IIA의 프로덕트 개발 이사 셔나 플랜더스(CRISC, CISA, CISM, SSGB, SSBB)의 토론에 근거하고 있다.
일반적으로 내부감사에서는 부정행위를 의심케 하는 패턴을 발견하고 부정행위 심사관에게 경고한다. 플랜더스가 제시한 사례의 경우 내부감사의 자동차 대출 검토가 포함되었다. 그녀의 팀이 취한 조치 중 하나는 연체 계좌를 평가하는 것이었다. 40개 계좌 중 5개가 눈에 띄었다. 시스템에는 사후 조치가 필요한 연체 대출을 표시하도록 설정되어 있었지만 어떤 이유에서인지 해당 5개 계좌가 표시되지 않았다. 게다가 이자율 0%, 만기 72개월, 최소지불금 없음 등 매우 이상한 특성을 갖도록 설정되어 있었다.
플랜더스는 조사를 통해 이 대출과 관련된 사용자 ID가 고객 서비스 담당자의 것이라는 사실을 발견했는데, 이는 있을 수 없는 일이었다. 이 역할을 맡은 사람은 일반적으로 대출을 승인하지 않는다. 그녀는 해당 대출과 관련된 로그 파일을 검토한 결과 각 대출의 신청 후 승인되기 약 1시간 전에 해당 사용자 ID 보유자에게 추가적인 시스템 액세스가 부여되었다는 사실을 발견했다. 이 액세스는 대출이 승인되고 활성화된 지 약 한 시간 후에 제거되었다. 비정상적인 대출 기간, 고객 서비스 담당자의 개입, 시스템 액세스 변경 등을 고려하여 감사팀은 이제 사건을 회사의 부정행위 부서에 넘겨야 할 때라는 것을 알았다.
조직의 정책 및 절차에 따라 의심스러운 활동에 대한 경고를 받았을 때 부정행위 부서가 취할 수 있는 조치는 다음과 같다.

- 감사인으로부터 받은 정보를 확증한다
- 해당 계좌와 관련된 전체 활동 범위를 조사한다
- 해당 5개 계좌의 생성이 단독적인 조치였는지 아니면 현재 진행중인 잠재적 사기계획의 일부인지 확인한다

• 공모자를 식별한다
• 다른 지점이나 사무소의 연루 여부와 전반적인 부정행위 범위를 고려한다

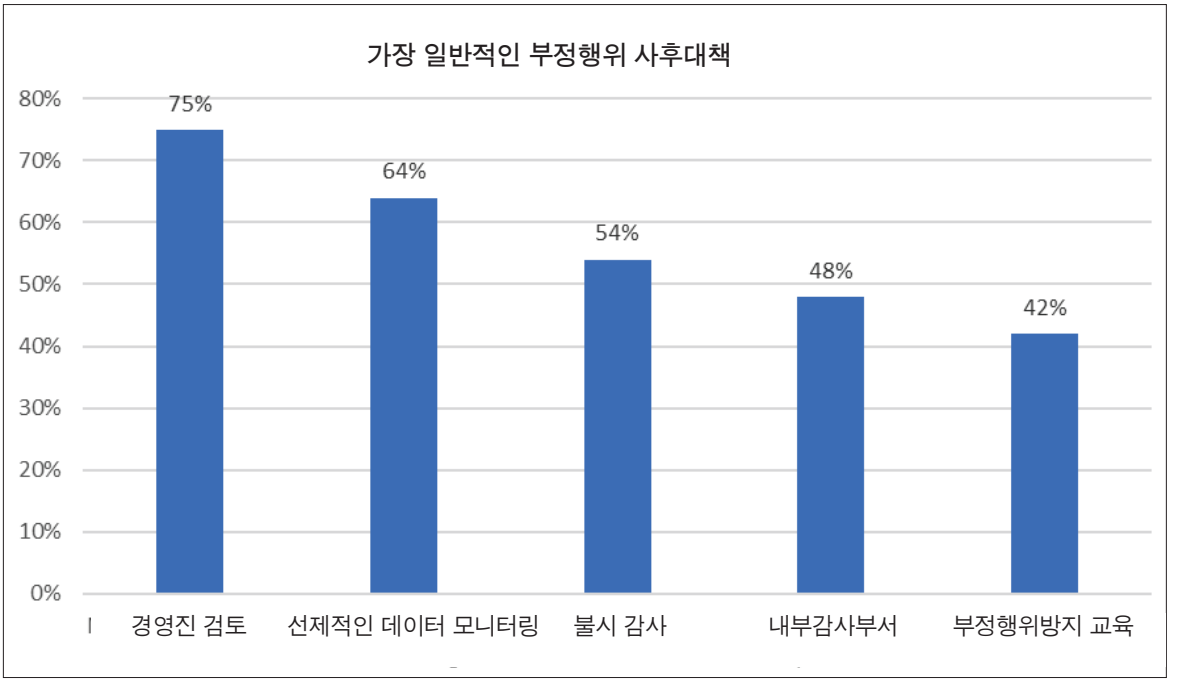
이 시점에서 사기 심사관은 부정행위를 중지시켜야 하는지 여부와 방법을 고려할 수도 있다. 더 많은 증거나 정보가 필요한 경우 부정행위를 일시적으로라도 지속하도록 허용하겠다고 결정할 수 있다. 웹세미나에 참석했던 ACFE의 연구 매니저 메이슨 윌더에 따르면 이는 회사가 이미 입은 손실액, 부정행위가 계속될 경우 잠재적으로 입을 수 있는 손실액, 조직의 리스크 선호도에 따라 달라지는 복잡한 결정이다. 이 경우 부정행위를 중단시키기 전에 취해야 할 단계에는 해당 고객 서비스 담당자와 면담하여 더 많은 정보를 얻고 부정행위의 범위를 파악하며 잠재적으로 추가적인 부정행위나 더 많은 부정행위를 발견하는 것이 포함될 수 있다.
증거를 수집하고 분석한 후 사기 심사관은 발견한 내용을 구두 또는 서면으로 조직 내 적절한 담당자에게 보고한다. 여기에는 경영진, 이사회 또는 감사위원회가 포함될 수 있다. ACFE 사기 심사관 매뉴얼(ACFE Fraud Examiners Manual)에 따르면 "부정행위 심사 보고서는 사기 심사관의 특정 활동, 심사 결과 및 적절한 경우 권고사항에 대한 설명이다." 그런 다음 조직의 경영진은 이 보고서를 사용하여 적절한 다음 단계를 결정할 수 있다.
사기 심사관이 상황을 검토하였으나 실제 부정행위를 발견하지 못한 경우, 원래의 위험 신호가 부정행위 리스크 관리 통제의 미비점으로 인해 발생했다고 판단하면 해당 건을 반송시킬 수 있다. 그러면 내부감사 보고서에 이러한 미비점이 포함될 수 있다.

강점의 결합

부정행위와 관련된 사람들은 경감이 중요하다는 점을 기억해야 한다. ACFE 설문조사 보고서는 부정행위를 적발하기 위한 사전 조치를 취하면 조기에 적발하고 손실을 줄일 수 있으며, 사후 조치를 취하면 부정행위가 장기간에 걸쳐 진행되어 피해자의 금전적 타격을 크게 만들 수 있다고 지적했다.
그러나 조직이 모든 부정행위 리스크를 식별하거나 제거할 수는 없다. 조직은 수많은 유형의 부정행위, 다양한 배후 동기, 광범위한 부정행위자를 만나게 된다. 그러나 경영진, 이사회, 직원 등 모든 수준의 사람들이 더 잘 알고 있을수록 합리적인 경감 노력을 전개하고 부정행위나 부정행위의 존재를 가리키는 위험 신호를 더 잘 식별할 수 있다. 내부감사인과 사기 심사관은 고유한 기술과 경험을 결합하여 조직의 전반적인 노력에 큰 기여를 할 수 있다. 조직은 이들의 업무를 활용하여 부정행위 리스크 관리 접근법에 대해 더 많은 정보를 바탕으로 결정을 내릴 수 있다.

재발 방지 대책

ACFE 설문조사에 참여한 조직 중 총 81%가 부정행위 발생 후 부정행위방지 통제장치를 수정했다. 아래 차트는 조직이 구현하거나 수정한 가장 일반적인 통제 변경사항을 보여준다. ACFE에서 권고하는 기타 부정행위방지 통제에는 자동화된 거래/데이터 모니터링, 감시 및 계좌 대사가 포함된다.



출처: *Occupational Fraud 2022: A Report to the Nations,* **the Association of Certified Fraud Examiners.**

마치며

거버넌스, 리스크 및 내부통제에 대한 제3의 검증 제공자로서 내부감사의 역할에는 객관적이고 독립적인 검증을 촉진하는 구조, 프로세스, 관행이 필요하다. 그러나 IIA의 3선 모델에서 언급했듯이 독립성은 고립을 의미하지 않는다.

3선 모델에 따르면 "내부감사의 업무가 관련성이 있고 조직의 전략 및 운영 니즈와 일치하는지 확인하기 위해 내부감사와 경영진 사이에 정기적인 상호작용이 있어야 한다. 모든 활동을 통해 내부감사는 조직에 대한 지식과 이해를 구축하며, 이는 신뢰할 수 있는 조언자이자 전략적 파트너로서 내부감사가 제공하는 검증과 조언에 기여한다."

이것은 내부감사와 공인사기심사관이 부정행위와의 전쟁에서 공통의 기반을 찾는 명백한 경우이다.

파트 3

후유증: 포스트 코로나 시대의 부정행위

전문가 소개

데이빗 도밍게즈(David Dominguez), CIA, CRMA, CPA, CFE

데이빗은 휴스턴에 위치한 이타포스(Itafos)의 감사 및 컴플라이언스 이사이다. 데이빗은 다양한 산업의 다국적기업과 협력하여 기업 및 지역 내부감사부서를 설립하고 지휘하며 변화시켜 왔다.

그는 북미, 라틴 아메리카, 유럽, 아시아에서 재무, 운영, IT 검증 및 자문 프로젝트를 주도하고 실행해 왔다. 또한 수많은 다중 관할권 수사, 데이터 애널리틱스 이니셔티브, 다양한 해외 주주, 합작 투자 및 공급업체 감사를 관리하고 참여해 왔다. 그의 전문 분야에는 기업과 조직 거버넌스, 전사리스크관리, 부정행위 리스크 관리, 2002년의 사베인즈 옥슬리법(Sarbanes-Oxley Act), 윤리 및 컴플라이언스 프로그램이 포함된다.

번역: 이은주(CIA)

- 삼성전자 내부감사팀 근무
- SC제일은행 내부감사부 근무
- 한국씨티은행 내부감사부 근무
- 2003~한국외국어대학교 통번역대학원 영어과 졸업
- 한-영 통역사, 제조, 금융, IT, 법률 등 다양한 분야의 한-영 통역사 활동

들어가며

지난 2년 동안 코로나19는 사람들이 일하는 방식, 일하는 장소, 조직이 공급업체와 공급망 문제를 처리하는 방식, 내부통제 유지와 부정행위의 탐지 및 예방과 같은 중요한 우려사항을 처리하는 방식에 이르기까지 전반적으로 혼란을 야기했다.

오늘날 최악의 팬데믹이 서서히 역사 속으로 사라지면서 세상은 숨쉬기 편해졌다. 하지만 그럼에도 불구하고 코로나19와 관련된 리스크가 더이상 걱정거리가 아니라고 예단해서는 안 된다. 실제로 그러한 예측을 한 조직은 심각한 실수를 저지르고 있는 것일 수 있다. 부정행위와 관련된 IIA의 3부작 시리즈 중 세 번째인 본고에서는 2022년 ACFE 국가 보고서에서 식별된 팬데믹과 관련된 다양한 부정행위 요인, 이것이 조직에 미치는 영향, 그리고 이러한 부정행위 리스크 요소를 경감하기 위한 노력에서 내부감사가 담당하고 있는 역할을 다루고 있다.

아직 남아있는 부정행위와 부정행위 리스크

팬데믹과 관련된 변화는 여전히 우려사항

코로나19에서 영감을 얻은 신종 사기의 등장

직장 내 부정행위에 관한 가장 최근의 국가 보고서에서 ACFE는 부정행위 발생 기간의 중앙값(즉, 부정행위의 시작 시점부터 탐지 시점까지의 일반적인 기간)이 12개월이라는 사실을 발견했다.[12] 이는 조직에 아직 발견되지 않은 팬데믹 관련 부정행위가 남아있을 수 있음을 뜻한다.

팬데믹과 관련된 변화가 계속해서 부정행위 리스크에 영향을 미치는 데는 여러 가지 이유가 있다. 예를 들어, 원격 근무 도입은 원래 임시적이었지만 많은 회사에서 표준 운영 절차로 전환되었다. 원격 근무는 종종 부정행위를 식별하거나 경감하기 위해 고안된 관행과 절차에 상당한 변화를 가져왔고 경우에 따라 절차가 느슨해졌다. 결과적으로, 팬데믹과 관련된 혼란이 줄어들었음에도 불구하고 이에 수반되는 리스크는 기업에 계속해서 위협을 가하고 있다.

내부감사는 팬데믹과 관련된 지속적인 부정행위 리스크를 처리하는 데 핵심적인 역할을 해왔고 앞으로도 계속할 것이다. 내부감사재단(IAF)과 크롤(Kroll)이 전 세계 IIA 회원을 대상으로 실시한 연구(study)에서 원탁회의에 참석한 많은 참가자들은 팬데믹으로 인해 "부정행위 리스크 관리와 관련하여 내부감사가 더 중요해졌다"고 느꼈다.[13]
여기에는 운영 과제에 대한 전략적 고려사항에 대한 추가적인 관여, 지속적인 검증 제공, 비즈니스 기능 전반에 걸친 협력 강화가 포함되며 동시에 감사인의 독립성도 유지해야 한다.

12 *Occupational Fraud 2022: A Report to the Nations*, ACFE.
13 *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.

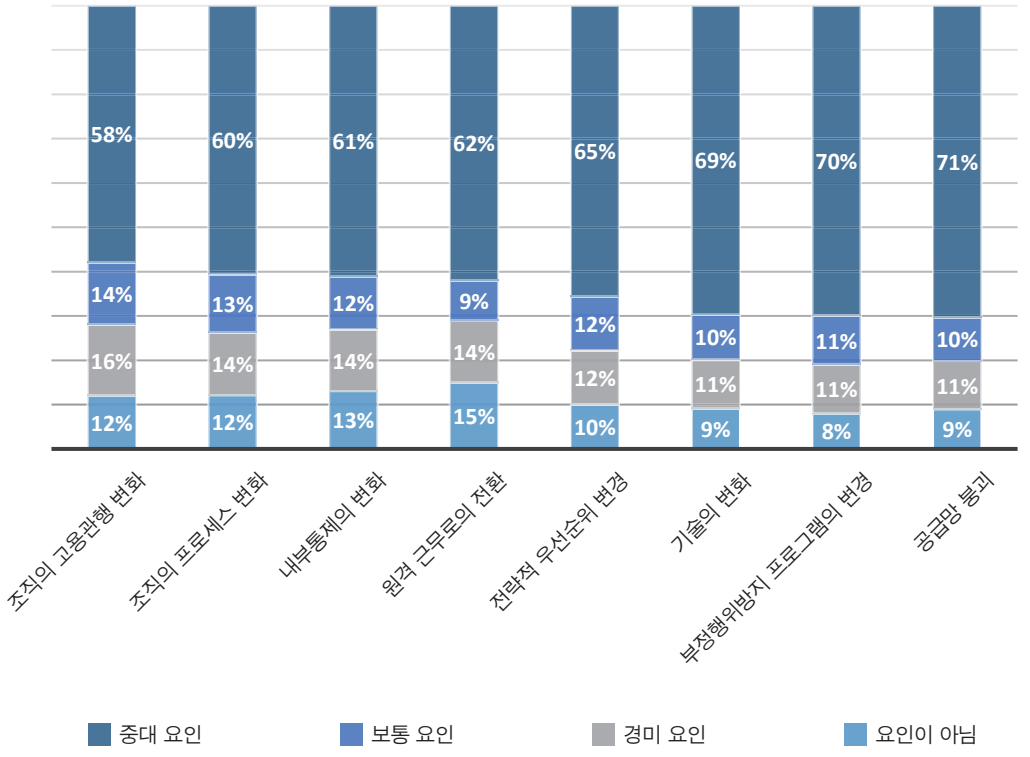
팬데믹과 관련된 부정행위 중 상위 리스크

고용관행의 변화, 원격 근무가 가장 큰 우려사항

절반 이상이 팬데믹 요인이 부정행위에 기여한다고 응답

ACFE는 직장 내 부정행위에 관한 보고서를 준비하면서 응답자의 52%가 자신이 조사한 부정행위 사건에서 팬데믹과 관련된 여러 이슈 중 최소 하나가 부정행위에 기여했다고 답한 것을 발견했다. 그중 팬데믹과 관련된 조직의 고용관행 변화가 가장 일반적이었다. 응답자의 총 42%는 고용관행의 변화가 직장 내 부정행위에 기여하는 중대, 보통 또는 경미한 요인이라고 답했다. 원격 근무로의 전환은 공통적으로 가장 중대하다고 언급된 요인이었으며(15%), 내부통제(13%)가 그 뒤를 이었다(그림 1 참조).

그림 1: 팬데믹과 관련된 요인은 직장 내 부정행위에 어느 정도로 기여했는가?



ACFE 보고서에서 확인된 팬데믹 관련 주요 이슈 중 일부를 심층적으로 살펴본 결과, 그 영향이 복잡미묘한 경우가 많다는 사실이 드러났다.

고용관행 변화로 인해 다양한 부정행위 리스크가 발생

팬데믹으로 인해 많은 조직은 직원의 직무 변경이나 확대, 업무 적응 시간이 제한적인 신규 인력의 투입 등 직면한 많은 혼란을 헤쳐나가기 위해 임시방편이나 지름길을 찾아야 했다. 또한, 팬데믹과 관련된 경제적 불확실성으로 인한 임시 해고나 휴가가 결국 영구적인 조치가 된 경우가 많다고 인산염 및 특수 비료 회사인 이타포스의 감사와 컴플라이언스 부문 이사 데이빗 도밍게즈가 말했다. "다양한 각도에서 확실히 리스크가 증가했다"라고 그는 말했다.

팬데믹으로 인한 업무 관행 및 프로토콜의 대대적인 조정과 조율, 그리고 새로운 업무를 수행하는 사람들의 잠재적인 학습 곡선을 고려할 때 조직은 이러한 변화가 의도하지 않은 영향을 미쳤을 가능성에 대해 생각해 보아야 한다. 고려 대상 영역은 다음과 같다.

문화

팬데믹으로 인해 기업 문화와 가치관을 재평가하고 재확인해야 할 여러 가지 이유가 있다.

팬데믹 기간 동안 "어떻게든 되게 만드는 것"은 미덕이었지만 이는 중요한 윤리적 관행과 태도가 일부 잊혀졌음을 의미할 수 있다. 신입 직원은 회사의 윤리적 가치에 대한 적절한 소개를 경험하지 못했을 수도 있다. 그렇다면 조직은 직원들에게 윤리적 행동에 대한 기대치를 상기시키는 것이 좋다.

ACFE는 보고서에서 "문화에 대한 적극적인 접근방식은 다양한 유형의 위법 행위를 방지하고 의욕과 생산성을 진작시킬 수 있는 행동을 촉진할 수 있다"라고 밝혔다. "문화는 직원의 업무 수행 방식, 품질, 컴플라이언스 및 기타 중요한 우려사항에 대한 결정 방법, 조직이 내부적으로나 외부적으로 어떻게 인식되는지에 영향을 미치는 강력한 능력을 가지고 있다."[14]

HR 고려사항

인력 부족과 하이브리드 및 원격 근무에 대한 정책 변화로 인해 익명의 내부 고발자 핫라인과 같은 오랜 HR 관행이 일부 변화되었다.

부정행위 예방을 위한 중요한 HR 수단 중 하나는 익명의 내부 고발자 핫라인이다. 실제로 ACFE 보고서에 따르면 부정행위의 42%가 제보를 통해 적발되었으며 다음으로 가장 일반적인 방법보다 3배 이상 높은 수치이다.

내부감사는 이 프로세스가 의도한 대로 작동하는지 여부를 조사하여 도움이 될 수 있다. 첫 번째 단계는 핫라인이 얼마나 잘 모니터링되는지, 불만 사항에 대해 후속 조치를 취하고 추적관리하는지 판단하는 것이라고 도밍게즈는 말했다. 그는 핫라인 모니터에게 다음과 같은 질문을 할 것을 권고한다.

- **직원은 핫라인에 어떻게 접근하는가?** 사무실의 건의함에 투서하거나, 핫라인 전화번호로 전화하거나, 온라인으로 불만사항을 신고하는 방법이 포함된다. 그러나 건의함과 핫라인 홍보 포스터는 원격 근무자에게는 도움이 되지 않는다는 점을 명심하라.
- **(해당 시) 핫라인을 여러 언어로 이용할 수 있는가?**
- **잘 추적되고 있는가?** 도밍게즈는 일부 회사에서 접수된 불만사항이 적은 것을 축하한다고 말했다. 이는 조직의 원활한 운영을 정확하게 반영하는 것일 수 있지만 핫라인 전화에 응답하지 않거나 불만사항을 수리하지 않은 결과일 수도 있다.

내부감사에서는 접수부터 해결까지 적절한 시기를 확인하고 후속조치 결정에 대한 근거가 충분한지 여부를 확인하기 위해 불만사항에 대응하는 프로세스를 검토할 수 있다. 조직에서는 신고에 뒤따를 보복에 대한 두려움 때문에 유효한 부정행위 제보를 놓치는 경우가 있다. 내부감사에서는 기업 핸드북이나 행동 강령이 보복행위를 명시적으로 금지하는지 여부를 검토할 수 있다. 더 나아가, 내부 고발자의 승진 불이익과 고과 평가 불이익 가능성을 회사가 추적하는 데 내부감사가 도움이 될 수 있다고 도밍게즈는 가리켰다. 불만사항이 입증되지 않은 경우에도 기업은 이에 대응하는 과정에서 업데이트나 설명이 필요한 정책을 찾을 수 있다고 그는 말했다.

14 *Assessing Corporate Culture: A Proactive Approach to Deter Misconduct*, Anti-Fraud Collaboration, March 2020

조직이 지속시키거나 구현해야 하는 기타 중요한 예방조치/통제장치는 다음과 같다.

- 신용 이력이나 기타 금전 문제 또는 임금 압류, 유치권 혹은 횡령 관련 판결 기록을 파악할 수 있는 신원 조회
- 자격증명 확인

ACFE는 사기범의 50%가 부정행위를 저지르기 전이나 저지르는 도중에 HR 관련 위험 신호를 하나 이상 나타냈다고 보고했다. 행동 단서 측면에서 볼 때, 자신의 소득수준 이상으로 생활하는 것은 2008년 이후 모든 ACFE 연구에서 가장 일반적인 위험 신호였다. 이는 39%의 사례에서 확인되었으며, 두 번째로 일반적인 요인인 금전적 어려움(25%)보다 훨씬 높다.

직업 관련 불확실성

ACFE는 부정행위에 기여할 수 있는 직업 관련 불확실성의 여러 사례를 확인했으며, 어려운 경제 상황은 그러한 불안을 가중시킬 수 있다. 구체적인 위험 신호에는 다음이 포함된다.

- 실직의 두려움
- 임금 인상이나 승진에서 탈락
- 복지 삭감
- 임금 삭감
- 비자발적인 근무시간 단축
- 좌천

팬데믹의 최악의 시기 이후 경제 환경은 안정되었지만 글로벌 비즈니스 환경에는 여전히 과제가 남아 있다. ACFE에 따르면 고용 불확실성과 관련된 이슈의 영향은 2022년에도 여전히 강했다. 이러한 불확실성 중 일부가 직원의 위법행위를 유발하는 요인이 될 수 있다는 점은 당연하다.

이러한 위험 신호는 일반적으로 직원에게 적용되지만 최고경영진에게 적용되는 몇 가지 추가적인 신호가 있다.

- **괴롭힘이나 협박**: 오너/임원의 경우 23%, 오너/임원이 아닌 경우 8%
- **통제 이슈**: 오너/임원의 경우 18%, 오너/임원이 아닌 경우 12%
- **"권모술수적(Wheeler-dealer)" 태도**: 오너/임원의 경우 17%, 오너/임원이 아닌 경우 9%
- **조직 내에서의 과도한 압력**: 오너/임원의 경우 13%, 오너/임원이 아닌 경우 6%
- **과거의 법적 문제**: 오너/임원의 경우 11%, 오너/임원이 아닌 경우 3%

코로나와 관련된 내부통제 상의 변화를 다시 생각해 볼 때

내부통제는 조직 전체의 조치와 결정이 정책, 보고 요건 및 컴플라이언스 의무에 부합함을 보장하기 위해 채택된 절차이다. 부정행위방지 통제를 통해 부정행위로 인한 손실을 줄이고 부정행위를 더 쉽게 감지할 수 있다. ACFE 연구에 따르면 부정행위 손실의 거의 절반은 내부통제 부족(29%)과 기존 통제의 무시(20%)라는 두 가지 요인으로 인해 발생한다. 내부통제를 구현하고 강화하는 것은 분명히 조직에 상당히 긍정적인 이점을 제공할 수 있다. 내부감사는 내부통제를 보고하고 개선사항을 권고하는 데 중요한 역할을 한다. 실제로 ACFE 설문조사에 따르면 내부감사부서가 없을 때 부정행위 손실의 중앙값이 50% 더 높은 것으로 나타났다(150,000달러 vs 100,000달러).

IAF/크롤 설문조사에 응답한 내부감사인들은 "원격 근무의 도전과제와 질병, 휴가, 인원 감축으로 인한 직원 감소 때문에 내부통제 프레임워크가 약화됐다"고 믿었다."[15]
위기 상황에서 조직에 새로 합류하는 사람들은 충분한 교육이나 인수 인계를 받지 못했을 수도 있고, 장기적인 프로세스와 통제가 포함되지 않은 비상 프로토콜만 배웠을 수도 있다고 도밍게즈는 말했다. "통제가 희석되었거나 균열이 생겼을 수도 있다"라고 그는 말했다. 그 과정에서 이러한 지름길은 원래는 특정 기간이나 특정 상황에서만 사용하도록 의도된 것이지만 표준 운영 절차가 될 수 있으며 앞으로도 계속 표준 운영 절차로 남을 수 있다.

이러한 우려는 많은 조직에서 긍정적인 변화를 가져왔다. 예를 들어 딜로이트(Deloitte)의 이사회효율성센터(Center for Board Effectiveness)와 감사품질센터(Center for Audit Quality)의 공동 설문조사(joint survey)에 응답한 감사위원회 위원 중 약 4분의 3은 원격 근무 환경 때문에 작년에 내부통제를 업데이트했다고 답했다.[16]

내부통제의 약점은 강력한 부정행위방지 조치를 무시하거나 무시하기 쉬운 환경을 조성하거나 조장함으로써 부정행위에 기여할 수 있다는 점이다. 예를 들어, 일반적이고 효과적인 부정행위방지 조치인 업무 분리(SOD)는 팬데믹 기간 동안 여러 위치에 흩어져 있는 직원들 때문에 수행하기 어려웠거나 인력 감축이나 부족으로 인해 무시되었을 수 있다. 이는 회사가 복원되어 효과적으로 작동하는지 확인하기 위해 지금 검토해야 하는 내부통제 유형이다.

내부감사는 중요한 프로토콜과 프로세스가 마련되어 있는지 확인하여 조직이 이러한 리스크를 해결하는 데 도움을 줄 수 있다. 프로세스 매핑 기술을 사용하면 최근 기간(6개월 또는 1년) 동안 프로세스를 추적하고 적절한 가이드라인이나 모범 사례와 다른 변형을 식별할 수 있다. 도밍게즈는 "표준 절차 또는 정책으로부터의 일탈을 확인하고 어떤 프로세스를 업데이트하거나 시행해야 하는지 식별할 수 있다"라고 말했다.
재검토해야 할 다른 영역으로 조달, 수표 작성, 은행 대사, 비용 환급 또는 재정적 고려사항과 관련된 모든 영역에 대한 내부통제가 포함된다.

여전히 중대한 부정행위 요인으로 남아 있는 원격 근무

사무실을 폐쇄하고 직원들이 집에서 업무를 수행할 수 있도록 허용하는 원격 근무로의 극적인 전환은 팬데믹 기간 동안 대부분의 조직에 가장 중요한 변화였을 것이다. 결과적으로 이 새로운 접근방식은 ACFE 보고서에서 부정행위에 크게 기여한 것으로 가장 많이 언급된 요소였다. 정상적인 상황에서 기업은 이러한 조치의 전략적 영향을 고려하는 데 몇 달이 걸릴 수 있지만, 이는 팬데믹 초기 몇 주 동안의 불확실성과 긴급성 때문에 본질적으로 불가능했다. 동료나 감독자의 눈으로부터 벗어나 혼자 일하는 것은 여러 형태의 부정행위를 저지르기 더 쉽게 만들 수 있다. ACFE에 따르면 원격 또는 하이브리드 근무로 영구적으로 전환하고 있거나 이미 전환한 사람들은 "해결하지 않고 방치할 경우 치명적인 결과를 초래할 수 있는 충돌선을 발견하기 위해" 변경 관리 계획수립에 참여해야 한다.[17]

---

15 *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge*, the Internal Audit Foundation and Kroll, March 2022.
16 *Audit Committee Practices Report: Common Threads Across Audit Committees*, Deloitte's Center for Board Effectiveness and the Center for Audit Quality, January 25, 2022.
17 *"Organizational Vulnerabilities in a Protracted Work -from-Home Scenario,"* Savita Nair, ACFE, January 12, 2023.

이 프로세스를 통해 내부감사에서 집중할 수 있는 몇 가지 잠재적인 충돌선이 있다. 예를 들어, IAF/크롤 보고서에 따르면 분산된 원격 환경에서 직원을 효과적으로 관리하는 데 따른 어려움과 이것이 문화에 미치는 영향이 해결해야 할 핵심 영역으로 언급되었다.[18] 윤리적 행동은 직장에서 이를 몸소 보여주는 다른 직원과의 상호 작용을 통해 학습되고 강화되는 경우가 많다. 경험이 더 많은 동료의 도움을 받으면 다른 직원이 부적절하거나 불법적인 행동을 하는 것처럼 보이는 혼란스럽거나 의심스러운 상황에서 직원이 대응하는 방법을 이해하는 데 도움이 된다.
특히 원격 근무와 관련된 부정행위 유형은 다음과 같다.

- **근태 불량이나 근무 시간에 대해 부정확하게 보고하는 행위**: 직접적인 감독을 받지 않을 때 직원은 이를 더 쉽게 저지를 수 있다.
- **데이터 도난, 기밀 정보 또는 민감한 정보의 오용 및 공유**: 직원의 기기에 접근할 수 있는 사람이나 원격 근무 시 데이터 오용에 대해 꺼림칙함이 덜한 직원이 저지를 수 있다.[19]

이와 관련된 우려사항은 원격 근무자가 부업을 갖는 것이다. 예를 들어, 직원은 원래 고용주를 위해 근무해야 하는 시간 동안 다른 회사에 대한 컨설팅이나 임시 업무를 수행할 수 있다고 도밍게즈는 말했다. 이는 엄연히 시간의 절도행위이며, 노트북이나 휴대폰과 같은 회사 자원을 오용하여 회사를 사이버보안 이슈에 노출시킬 수도 있다. 또한 부업은 직원이 경쟁사를 위해 일하는 경우, 특히 경쟁사에 유익한 정보를 공유하는 경우 이해 상충을 야기할 수 있다. 내부감사는 직원이 받는 교육 유형과 직원 핸드북 및 정책이 새로운 근무 환경에 맞게 업데이트되었는지 질문함으로써 이 문제를 해결하는 데 도움이 될 수 있다고 도밍게즈는 말했다.

기술 변화로 인해 발생하는 부정한 거래

기술을 통해 조직은 내부통제 및 원격 근무와 같은 영역에서 효과적인 절차를 구현할 수 있다. 조직은 이미 사이버보안 우려를 해결하기 위해 기술 개선에 투자하고 있었으며, 팬데믹으로 인해 기업은 시스템 개선을 가속화하고 강화했다. 기술 업그레이드에 많은 내부감사 부서가 포함되었다. 실제로 내부감사인의 29%는 팬데믹이 시작된 이후 부정행위 및 부패를 식별하는 도구로 데이터 분석을 추가했다.[20]

동시에 기술 도구를 오용하거나 무시하면 부정행위의 모의가 더 쉽게 성공할 수 있다. 앞서 언급했듯이 데이터 절도는 원격 근무와 관련된 우려사항 중 하나이다. ACFE에 따르면 데이터 절도 리스크에 대한 솔루션으로 직원에게 홈 네트워크를 보호하고 가족과 공유하지 않도록 요구하는 것이 포함된다. VPN을 사용하고 보다 강력하고 복잡한 비밀번호와 설정을 사용해 가정용 컴퓨터를 보호하는 것도 중요하다. 다른 옵션으로는 다중 인증(MFA)과 데이터 보안 및 개인정보보호에 대한 직원 연례 교육이 있다. 또한 조직은 허용가능한 전자 기기, 소셜 미디어 및 회사 데이터 사용에 대해 정책을 수립해야 하며 직원이 이러한 정책을 열람하고 이해했음을 확인하도록 요구해야 한다.

원격 또는 하이브리드 환경에서 작업하는 조직은 또한 직원이 가정용 기기에서 소프트웨어 및 보안 패치를 업데이트하도록 해야 할 뿐만 아니라 피싱과 기타 해킹 위협을 방지하는 최선의 방법에 대해 직원에게 교육해야 한다.[21] 물론, 팬데믹의 영향을 따라잡기 위해 노력하고 있는 기업들은 자체적으로 사이버보안 조치를 검토하여 최신 상태를 유지해야 한다.
이러한 우려를 해결하기 위해 도밍게즈는 내부감사를 통해 어떤 보안 프로토콜이 마련되어 있는지, 조직에서 사용하는 데이터 절도 방지 수단은 무엇인지, 다중 인증 및 VPN이 필요한지, 직원의 퇴사 시 신속하게 계정이 비활성화되는지 조사할 수 있다고 권고했다.

컴플라이언스와 윤리 노력에 영향을 미치는 "심리적 퇴사(Quiet Quitting)"

"심리적 퇴사"는 근로자가 최소한의 업무 요구사항만 수행하는 행위를 뜻한다. 갤럽(Gallup)의 추정에 따르면 이러한 근로자는 미국 노동 력의 최소 50%를 차지한다. 심리적 퇴사 행위에 참여하는 근로자의 수준은 32%인 반면, 적극적으로 참여하지 않는 근로자의 수준은

18%였다. 갤럽은 이러한 태도가 협업하는 업무가 많거나 고객의 니즈를 충족하기 위해 추가적인 노력이 필요할 때 특히 문제가 된다고 지적한다. 심리적 퇴사 경향이 많은 주목을 받고 있지만, 고용주는 큰 소리를 내고 그만두는 사람, 즉 자신의 불만을 적극적으로 표현하고 퍼뜨리는 사람도 여전히 존재한다는 점을 인식해야 한다.[22]

이러한 추세는 생산성, 효율성 및 직원 유지에 나쁜 소식이 될 수 있다. 동시에 리스크 관리에도 부정적인 영향을 미칠 수 있다. "사람들은 자신이 응당 기울여야 하는 주의를 기울이지 않는다"라고 도밍게즈는 말했다. 그리고 기업 컴플라이언스 인사이트(Corporate Compliance Insights)가 지적한 것처럼, 컴플라이언스 및 윤리 프로그램이 성공하려면 조직 내 모든 사람의 참여와 지원이 필요하다. "업무에 대한 상대적으로 부정적인 전망과 최소한의 업무만 수행하겠다는 마음가짐이 결합되면 컴플라이언스 및 윤리 전문가가 사람들이 이슈를 제기하는지 확인하기 위해 의존하는 추가적인 무언가가 사라진다."[23]

이는 부정행위 리스크 관리 프로그램에서도 마찬가지이다. 직원은 승인 및 거래에 대해 건성으로 결재하거나 이상징후를 무시할 수 있고, 이상한 점을 에스컬레이션했으나 이들의 직속 상사가 이미 심리적 퇴사 상태라 이상징후를 무시할 수도 있다.

내부감사는 직원 만족도 조사, 이직률 조사, 퇴사 인터뷰를 실시하여 직원의 참여에 대한 문제점을 파악할 수 있다. 도밍게즈는 최근 추세를 코로나 이전의 활동과 비교하여 팬데믹이 어떤 영향을 미쳤는지 이해할 수 있다고 말했다.

---

18 *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge,* the Internal Audit Foundation and Kroll, March 2022.
19 *"Organizational Vulnerabilities in a Protracted Work -from-Home Scenario,"* Savita Nair, ACFE, January 12, 2023.
20 *Fraud and the Pandemic: Internal Audit Stepping up to the Challenge,* the Internal Audit Foundation and Kroll, March 2022.
21 *"Organizational Vulnerabilities in a Protracted Work-from-Home Scenario,"* Savita Nair, ACFE, January 12, 2023.
22 *"Is Quiet Quitting Real?"* Jim Harter, Gallup Workplace, September 6, 2022.
23 *"Why 'Quiet Quitting' Could Harm Ethics and Compliance Functions,"* Lisa Beth Lentini Walker, Corporate Compliance Insights, September 14, 2022.

마치며

이 모두가 합쳐지면 무엇이 될까? ACFE에 따르면 조직은 매년 부정행위로 인해 약 5%의 매출 손실을 입으며, 손실액의 중앙값은 117,000달러, 평균은 1,783,000달러이다. 일반적으로 부정행위로 인한 손실은 월 평균 8,300달러에 이른다.
이는 모든 조직에서 심각한 고려사항이다.

최악의 팬데믹 상황과 그 이후로 조직은 전략적 의사 결정자가 운영 프로세스를 재평가하고 개선할 수 있도록 내부감사인에게 의존해 왔다. 이러한 관행은 특히 부정행위방지 내부통제를 평가할 때 계속되어야 한다. 세계는 팬데믹에서 벗어났을지 모르지만 팬데믹과 관련된 부정행위 위협을 모두 떨쳐버린 것은 아니다.

팬데믹이 시작된 이후 내부감사가 부정행위를 경감하거나 중지하는 데 기여할 수 있다는 점에 대한 인식이 더욱 커졌다.
과거에는 부정행위가 이미 발생한 후에 내부감사가 진행되는 경우가 많았다.
이것은 변화하고 있다. 이제 조직은 부정행위를 적발할 때까지 기다리거나 너무 많은 피해가 발생하기 전에 해결되기를 기다리지 않을 것이다. 그를 위해 조직은 예방 기반 대화에 내부감사인을 참여시키고 있다. 즉, 부정행위가 발생하기 전에 부정행위방지 통제를 고려하도록 요청하고 있다고 도밍게즈는 말했다. 내부감사에서는 또한 부정행위 리스크 평가 및 부정행위 리스크 평가 프레임워크에 대한 논의를 촉진하고 이러한 평가와 통제 테스트의 빈도와 효율성을 고려하고 회사의 상시 리스크 프로파일에 발생한 변경사항을 기록한다. 도밍게즈는 "내부감사인은 부정행위 적발을 기다리는 대신 예방하는 측면으로 이동하고 있다"라고 말했다.