Deloitte.

Internal audit insights

High-Impact areas of focus – 2016

이사회와 경영진을 비롯한 이해관계자들은 내부감사에 기존보다 훨씬 많은 역할을 기대하고 있습니다. 기존의 내부감사방식은 중요하지 않은 영역에 지나치게 많은 자원을 투입하기도 하고, 반대로 매우 중요한 영역을 상대적으로 소홀히 다루기도 합니다. "중요한 영역"의 정의는 기업이 속한 산업이나 비즈니스 모델, 노출된 리스크, 지역, 규제환경 등에 따라 달라질 수 있을 것입니다. 그러나, 일반적으로 중요성이 적은 영역에 대해서는 이미 시스템이나 통제가 잘 구축되어 있고, 그에 관한 리스크나 이슈도 잘 알려져 있습니다. 이러한 영역 또한 내부감사가 관심을 가져야 하지만, 그 때문에 중요한 영역에 투입해야 할 내부감사 자원이 분산되어서는 안 됩니다.

본 "High-Impact areas of focus"에서 딜로이트는 11 개의 중요 영역을 2016 년 내부감사 계획을 수립할 때 고려할 절차들과 함께 제시합니다.

1. Cyber Security
2. Key Performance Indicator assurance
3. Internal Audit Analytics
4. Data Visualization (시각화)
5. Corporate Governance
6. Dynamic Internal Audit Planning (동적인 내부감사계획수립)
7. Crisis Management Planning (위기관리계획)
8. Data Governance & Lifecycle Management (데이터 거버넌스와 수명주기 관리)
9. IT Internal Audit
10. Vendor Governance (협력사 관리)
11. International Professional Practices Framework (국제 업무기준)

1. Cyber security

정보보안감사의 효과성을 높이기 위해서는 내부감사에서 사이버 리스크를 어떻게 정의하는지가 매우 중요합니다. 여전히 웹 보안, 데이터 접근보안, 방화벽 등 특정 분야에 한정된 감사들이 "정보보안감사"라는 이름으로 수행되고 있습니다. 이러한 감사접근방식도 일정한 수준의 확신을 제공할 수는 있으나, 정보보안과 관련해서 조직이 직면한 전체적인 리스크를 다루지 못할 수 있습니다. 정보보안의 정의는 포괄적이어야 하고, NIST, ISO, COSO and ITIL[1]등의 표준과 프레임워크에 기반하여야 합니다. 또한 정보보안은 모든 디지털 자산은 물론, 데이터를 생산, 저장, 분석하고 전송하는 프로세스와 시스템까지도 다루어야 합니다. 정보보안은 이제 이메일, 문자메시지, 소셜미디어, 빅 데이터, 웹 등으로까지 확장되었습니다. 이렇듯 정보보안이 과거 어느 때보다도 중요해지면서, 조직이 갈수록 진화하는 정보보안 위협에 지속적으로 대비(vigilant)하고 있는지, 사고 발생 시 회복(resilient)할 수 있는 역량을 확보하고 있는지도 내부감사가 평가하여야 합니다.

Steps to consider:

- 리스크 관리의 3 단계 방어선으로서, 내부감사는 1 단계 방어선(현업)과 2 단계 방어선(리스크 관리)이 취하는 절차가 기존 및 예상되는 정보보안 리스크들을 다루기에 충분한 지를 확인하라[2].
- 아직 진행되지 않았다면, 내부감사조직에서 정보보안 위협의 예방, 탐지 및 복구를 포함한 강력한 프레임워크에 기반한 정보보안 리스크 평가를 통해 리스크 기반의 감사계획을 수립하라.
- 정보보안 감사계획을 세울 때에는 정보보안 리스크 프로파일(누가, 어떤 이유로, 어떤 정보자산을 공격할 것인지)를 고려하라. (조직에 따라 다르겠지만, 데이터 보호, 벤더 관리, 정보보안 사고 관리, 복구 등이 리스크가 큰 영역에 포함될 수 있음).

리스크 기반의 정보보안 리스크 평가를 수행하기 위해서는 수년간의 반복적인 노력이 필요합니다. 정보보안감사는 내부감사 역량의 지속적인 개선과 함께 IT 및 정보보안, 사업 단위 및 리스크 관리까지 이르는 조직 내 다양한 임직원과의 긴밀한 협조와 적극적인 참여가 필요합니다.

[1] NIST: National Institute of Standards and Technology (미국 국립표준기술원) / ISO: International Organization for Standardization (국제표준화기구) / COSO: Committee of Sponsoring Orgnizations of the Treadway Commission (COSO 위원회: 내부통제, 전사적위험관리 등의 통합프레임워크 제정기관) / ITIL: Information Technology Information Library (영국에서 개발한 IT 관리 가이드라인)

[2] 3 단계 방어선 모형(또는 3 차 방어선 모형; Three Lines of Defense) 참조

2. Key Performance Indicator (KPI) assurance

고객관계, 제품 품질, 지속가능경영, 리스크 관리 등은 경영진이 비재무적 KPI를 활용하는 대표적인 분야입니다. 비재무적 KPI를 측정하고 관리하기 위한 프로세스와 시스템, 통제는 재무적 KPI에 비해 훨씬 뒤떨어져 있습니다. 이는 곧, 감사기법과 방법론을 KPIs에 잘 적용시킬 수 있다는 의미가 되기도 합니다. 감사의 시각에서 KPI에 접근함으로써 관련 프로세스, 시스템 및 통제를 개선할 수 있습니다. 경영진이 KPI 측정치를 근거로 제시하는 보고서나 공시자료들을 주기적으로 발행하기 때문에 KPI를 검토하는 것 또한 이 중요한 영역이 됩니다. 예를 들면, 에너지 및 용수 사용량 혹은 고용 및 근로조건에 관한 보고서나 고객 서비스나 제품 품질에 대한 발표자료 등은 정확하고 신뢰할 수 있는 KPI를 필요로 합니다. 이러한 KPI를 검증하고 확인할 수 있는 가장 적합한 조직이 바로 내부감사입니다.

Steps to consider:

- 내부감사가 KPI에 집중해서 효과를 얻을 수 있는 영역이 어디인지 확인
- 지속가능 경영보고서(sustainability reports)나 감독당국에 제출된 보고서에 사용된 KPI, 혹은 서비스 가용성이나 정시 배송 등 이미 시장에 제시한 약속과 관련된 KPI를 고려
- 그러한 KPI의 기초가 되는 프로세스 및 시스템에 감사 전문지식을 적용

경영진이 특정한 측정치를 위해서 적합한 KPI를 추적하고 있는지, 관련되는 프로세스는 잘 설계되었고 통제되고 있는지를 먼저 확인 후, 데이터와 프로세스에 대한 확신을 제공할 수 있습니다.

3. Internal audit analytics

표본조사에만 의존한 사후 적발위주의 감사는, 신규 리스크나 조직 전략과의 적합성, 성과 개선 등의 영역에서는 이해관계자의 요구사항을 충족할 수 없기 때문에 분석(analytic) 기법이 요구됩니다. 다행히도 최근의 분석 툴들을 활용해서 전체 모집단을 분석하는 데에는 고도의 전문성이 필요하지는 않습니다. 예를 들면, 특정 사업부문의 주문이나 청구서, 대금지역 내역 등을 전수를 조사한다면, 수 백 건의 거래를 표본조사 하는 것보다 더 많은 오류나 부정 혹은 내부통제 위반 사례들을 찾아 낼 수 있고, 예외적인 사안에 대해서는 추가적으로 깊이 있는 조사도 가능합니다. 또한 대용량 데이터에 리스크 요인을 적용해서 표본조사 방법으로는 놓칠 수 있었던 리스크를 발견할 수도 있습니다. 내부감사 조직이 분석기법의 도입을 머뭇거리는 것은 주로 그 효과를 과소평가하거나, 이를 활용하는 것을 지나치게 어렵게 생각하거나 혹은 변화를 두려워하기 때문입니다. 하지만, 애널리틱 기법을 도입한 조직에서는 내부감사의 영역이 확장되고 효율성과 효과성이 개선되며, 내부감사를 통해 더 많은 가치를 창출하는 효과를 누리고 있습니다.

Steps to consider:

개인 비용분석이나 구매 거래 분석 등 곧바로 성과를 낼 수 있는 영역에 범용 애널리틱 기법을 적용하는 것부터 시작하여, 관련 정책이나 규정을 잘못 이해하거나 우회한 사례 혹은 내부통제를 우회한 사례가 있는지 확인하고, 비용의 낭비를 막고 과오 지급된 금액을 회수할 수 있는 다른 기회까지도 모색합니다.

산업에 따라 (예를 들어 은행업의 경우) 감독당국에서 미래 지향적인, 즉 애널리틱 기법을 활용한 감사가 필요한 부분을 식별할 수도 있습니다. 향후에는 내부감사가 특정한 분석 작업을 관련 사업부문이나 기능으로 이관하여 리스크 관리에서의 1 차 방어선 역할을 개선할 수도 있을 것 입니다.

4. Data visualization (시각화)

시각화는 데이터를 분석한 결과를 버블 차트(bubble charts), 히트 맵(heat maps), 쌍방향그래프(interactive graphs) 등의 시각적인 형태로 변환하여 전문 분석가가 아닌 사람도 쉽게 이해할 수 있게 만들어 주는 것입니다. 시각화 툴은 차트 라이브러리에서 사용자가 직접 설정하는 요약 자료(dash board) 등까지 다양한 기능들을 제공하는데, 사용 상의 복잡성이나 도입비용이 크게 하락하고 있습니다. 시각화를 통해, 감사범위를 수립할 때 리스크가 큰 영역이나 내부감사가 특별히 집중할 영역을 정확하게 짚어내어 감사자원을 효과적으로 배분할 수 있습니다. 감사진행 단계에서는 전통적인 방법으로는 식별하기 어려운 추세나 패턴, 혹은 예외사항 등을 도식적으로 제시함으로써, 관련 거래에 대한 정밀조사를 진행할 수 있습니다. 마지막으로, 시각적인 형태의 데이터는 이해하기가 더 쉽기 때문에 보고단계에서 이해관계자의 기대를 충족할 수 있습니다.

Steps to consider:

- 시각화 도구들에 관심과 소질이 있는 한 두 명의 직원들을 훈련
  - 좋은 분석 툴들의 데스크 탑 라이선스 버전은 가격도 상대적으로 저렴하고, 데이터를 해당 패키지에 upload 하는 것도 어렵지 않음.
- 특정한 영역의 감사범위 설정, 감사 수행, 결과 보고 등에 시각화를 적용
  - 시각화는 이사회나 감사위원회 보고용 자료에도 큰 의미가 있음.
- 초기 시험적용 단계에 시각화 툴에 대한 경험을 보유한 인력의 참여
  - 전문성을 활용하고 새로운 도구의 도입에 따른 일반적인 오류도 회피할 수 있음.

5. Corporate governance

내부감사는 지배구조를 보다 효과적으로 변환하는 것을 지원할 수 있습니다. 지배구조에서의 내부감사 3 원칙은 비례성(proportionality), 객관성(objectivity), 특수성(specificity)입니다. 먼저 '비례성'이란, 내부감사가 조직의 성숙도나 산업, 규제환경뿐만 아니라 규모, 사업 내용, 복잡성 등을 함께 고려해야 한다는 것입니다. 객관성은 Deloitte 의 Corporate Governance Framework 과 같은 외부 프레임워크나 감독기관의 규정을 고려해야 한다는 원칙이며, 특수성이란 내부감사가 현업 업무의 진행방식과 행동에 집중하여야 한다는 원칙입니다.

Steps to consider:

- 조직의 지배구조 프레임워크를 검토하고, 그 결과에 따라 감사계획을 수립
  - 내부감사가 조직 내 이사회나 경영진의 운영현황을 선진 사례와 대비해서 평가하고, 이사회나 경영진의 자가평가 결과를 선진사례와 비교해서 검토할 수도 있음 (지배구조의 효과성에 대한 감사에는 평가 대상과 함께 평가 영역이 포함되어야 함.)
  - 평가영역에는 일반적으로 지배구조, 전략, 운영, 계획 수립, 성과평가, 윤리성, 역량, 리스크, 문화, 법규 및 규정준수, 보고절차 등이 포함될 수 있음.

이러한 영역에 대한 감사를 통해 내부감사는 이해관계자들에게 이사회나 경영진의 성숙도와 효과성에 대한 확신을 제공할 수 있고, 이사회와 경영진에게 지배구조를 개선할 방안을 제시할 수 있습니다.

6. Dynamic internal audit planning

동적인 내부감사 계획수립은 정적인 혹은 순환원칙에 의한 내부감사계획에서 크게 발전한 방식으로, 정성 혹은 정량적인 방법을 활용해서 이슈를 식별하고, 핵심 이슈에 내부감사 자원을 할당하는 주기적 혹은 지속적인 과정입니다. 위기와 기회는 갑자기 다가오기 때문에 내부감사가 반드시 다루어야 할 요소입니다. 동적인 계획수립은 데이터분석과 상시모니터링(자동화된 데이터 수집을 통한)을 활용하여 연간 리스크 평가절차를 보완하는 유연한 접근방법입니다. 동적인 계획수립은 내부감사의 미션인 확신의 제공과 조언 및 예측을 모두 가능하게 합니다. 즉, 내부감사의 효율성을 높이고, 내부감사가 경영진에게 리스크에 대한 조언을 제공하고 개선사항이나 리스크 경감 전략을 제공하며, 새로운 리스크와 기회요인을 예측할 수 있도록 합니다.

Steps to consider:

- 동적인 내부감사 계획수립을 위해서는, 내부감사인들이 재무에 관한 프로세스, 시스템 및 내부통제에 대한 지식만큼 전략이나 사업, 운영 및 리스크 이슈에 대한 전문성을 보유하고 있어야 합니다. 또한 계획을 수립하고, 계획의 수정에 부담을 느끼지 않으며, 새로운 요구사항에 신속하게 반응할 수 있는 유연성도 필요합니다. 예를 들어, 내부감사는 규제환경 혹은 시스템과 내부통제를 통합하는 것과 관련된 이슈 등과 같은 가치창출을 저해하는 리스크와 방해요소들을 식별함으로써 인수합병 과정을 지원할 수 있습니다.
- 또한 인공지능(artificial intelligence)이나 리스크 감지기법(risk sensing technologies)의 발전으로 동적인 내부감사를 지원할 수 있습니다.

7. Crisis management planning [위기관리계획]

비즈니스의 세계화와 가상화(virtualization)는 소셜 미디어가 평판 리스크를 증폭시켜서 모든 위기들이 광범위한 영향을 미칠 수 있다는 것을 의미합니다. 여전히 "위기 준비"를 영속성관리(business continuity)이나 비상 대응 혹은 재해 복구 정도로 국한시키는 내부감사 조직이 많습니다. 오늘날의 위기관리계획은 이러한 요소들을 통합해서 하나의 광범위한 대응계획을 구현하여야 합니다. 또한, 위기관리계획은 내부 및 외부 커뮤니케이션은 물론, 필요하다면 이해관계자들에게 확신을 제공하고 경영진이 위기에 대응할 수 있도록 전세계적인 협력방안도 고려해야 합니다.

Steps to consider:

감사계획을 통해 경영진이 모든 잠재적인 위기와, 그 위기들이 조직에 미칠 수 있는 영향을 파악하고 있는지를 확인할 수 있습니다. 자연재해이건 인재이건, 물질적인 것이건, 가상의 무형적인 것이건, 지역적인 것이건, 멀리 떨어져 발생한 것이건, 위기는 조직의 운영이나 임직원, 공급망, 공장이나 기계장치, IT 설비나 데이터를 위태롭게 만들 수 있습니다. 감사계획은 경영진이 모든 영향을 평가한 결과에 기초해서 통합적인 계획을 수립했는지를 확인하여야 합니다. 그래야 감사주기마다 2-3 개 정도의 분야에 집중하여 위기관리계획의 깊이나 대응성, 통합성을 평가할 수 있습니다. 위기관리역량이 상대적으로 성숙하지 않은 조직에서의 내부감사는 확신을 제공(assurance)하는 것보다 자문(advisory)에 초점을 둘 수도 있습니다.

8. Data governance & life cycle management (데이터 관리)

대부분의 조직들은 일정한 형태의 데이터 거버넌스를 필요로 합니다. 세부적인 사항은 해당 조직과 그 조직이 속한 산업에 따라 달라질 수는 있지만, 데이터 거버넌스는 대체로 누가 데이터를 소유하고, 누가 어떤 목적으로 데이터를 이용하며, 또 데이터가 신뢰성과 정확성을 확보하고 있는지 등에 관련된 정책과 절차들을 포함합니다. 또한 데이터의 유실이나 도난을 예방하고 적절하게 파기하기 위한 관리나 안전장치 등도 포함됩니다.

리스크는 전형적으로 개인정보나 규제 및 평판 관련 이슈에서 발생하는데, 고객 데이터의 유실이나 도난이 이들 이슈의 공통적인 관심사입니다. 내부감사는 데이터 거버넌스에 대한 조직의 필요성에 따라 그 노력을 달리 하여야 합니다. 예를 들어 금융 서비스, 생명과학, 소비재, B2B 기업들이 데이터를 이용하는 방식은 서로 다르기 때문에 데이터 거버넌스에 대한 차별화된 접근방식이 필요합니다.

Steps to consider:

- 가장 중요한 데이터와 고위험 데이터에 집중하라.
- 데이터 수명주기와 관련된 정책과 절차를 검토하고, 이러한 정책과 절차가 의도한대로 이행되고 있는지를 검토하라.
  - 데이터를 수집, 저장, 사용 및 파기하는 정책과 절차 및 접근을 통제하고 정확성을 담보하기 위한 정책과 절차 등
- 관련 정책과 절차가 존재하지 않거나, 기초적인 정책 혹은 절차만 존재하는 사업부문에 대해 자문과 개선을 위한 방향성을 제시하라.
- 데이터의 품질만을 판단하지 말고, 바람직하거나 요구되는 수준의 데이터를 생성하고 보호하기 위해 필요한 프로세스와 통제에 집중하라.

9. IT internal audit

IT 와 관련한 이슈들은 이제 기술로 인해 야기되는 사업의 중단뿐만 아니라 소셜미디어, 빅데이터 및 앱(apps)까지 포함합니다. 그렇지만 IT 내부감사는 여전히 10 년 전과 크게 달라진 것이 없어 이해관계자들이 IT 감사를 외면하기도 합니다. Sarbanes-Oxley (SOX)의 요구사항 준수나, 재해복구 등에 대한 감사도 반드시 필요하지만, 이러한 영역에 대한 감사 때문에 내부감사 자원이 부족하여 새로운 정보기술 리스크를 놓쳐서는 안됩니다. 감사보고서가 충분한 가치를 제공하지 못하면 지속적으로 내부감사 자원의 제약이 따를 것입니다. 리스크와 가치에 기반해서 감사계획을 수립하면 어떤 영역에 내부감사 자원을 투입할 것인지를 결정할 수 있습니다. 70% ~ 80 %의 감사자원을 리스크가 낮거나 창출할 수 있는 가치가 적은 영역에 투입하는 경우가 너무 많습니다.

Steps to consider:

기술이 발전하는 속도와 디지털 자원의 가치를 생각할 때, 균형 잡힌 내부감사 접근법이 필요합니다. IT 내부감사 활동을 핵심영역, 선진기술영역, 신규기술영역 등 세 가지 영역으로 그룹화하여 IT 자원을 이 세 영역에 균형있게 배분하여야 합니다.

- 핵심영역: 과거 수 년간 진행되어 온 영역(예: SOX 테스트)
- 선진 기술영역: 계속 다루어 왔으나 전통적으로 IT 내부감사의 핵심은 아닌 영역
- 신규 기술영역: 새롭고, 잠재적으로 파괴적일 수 있는 기술을 포함한 영역

10. Vendor governance [협력사 관리]

제 3 자와의 관계는 많은 효익을 제공하는 반면 리스크도 수반하며, 리스크에 대한 책임은 아웃소싱할 수 없습니다. 제 3 자 리스크는 조직 내의 다양한 사업부문과 기능에 걸쳐 있어서 계약구조를 파악하기도 어렵고 계약 내용을 준수하기 위해 전향적이고 예방적인 접근법을 취하기가 어렵습니다. 제 3 자 관계의 전체 가치를 실현하는 것을 지향하여 협력사와의 계약서와 KPI 를 검토하면 보다 완전한 그림을 그릴 수 있을 것입니다.

대부분의 계약에 감사권에 대한 조항이 들어가 있지만, 구체적인 내용은 다양하고 "감사"를 수행하는 인력들이 특수한 비즈니스 모델과 복잡한 계약조항을 평가하는데 필요한 역량이 부족할 수도 있습니다. 협력사들이 특정한 통제나 서비스에 대한 보고서를 제공할 수도 있지만, 이런 보고서들은 너무 일반적인 내용이거나 계약 상의 요구사항에는 미치지 못하는 수준일 수 있습니다.

Steps to consider:

내부감사가 협력사 관리에 일찍 관여할수록 좋습니다. 예를 들어, 협력관계가 제대로 작동하고 있는지를 일년 단위가 아니라 분기별로 내부감사가 확인할 수도 있습니다. 계약 초기에 관련 내용들을 명확하게 하는 것이 서로의 관계를 원활하게 유지되도록 합니다. 많은 협력업체들은 장기간이 소요되는 사후적인 복구과정보다, 오류나 계약 해석과 관련한 이슈를 조기에 통지해 주기를 원합니다.

데이터 애널리틱은 전수 거래를 검토해서 추가적인 조사가 필요한 예외적인 사항들을 발견하는데 큰 도움이 될 수 있습니다. 몇몇의 중요한 관계에 대한 실제 사례를 통해 내부감사가 계약관계를 확인하는 것의 가치를 입증할 수 있습니다. 즉 감사인들은 그들의 역량범위 내에서 감사업무를 수행하면서, 계약의 준수와 이행여부를 평가하기 위한 전문적인 역량이 언제 필요한지 판단하여야 합니다.
일반적으로 제 3 자와의 계약 부분에서 일부 부족한 투명성을 용납하면서 많은 기회를 놓치곤 합니다. 이런 기회들을 찾아내는 것은 계약 당사자 모두의 권리이며, 내부감사가 측정가능한 가치를 제공할 수 있는 영역이기도 합니다.

11. International Professional Practices Framework [업무수행기준]

내부감사협회(The Institute of International Auditors, IIA)는 2015 년 7 월, 국제업무수행기준(IPPF; International Professional Practices Framework)을 개정하여 내부감사의 진화하는 역할을 반영하였는데, 이는 1999 년 이래 최초로 이루어진 대규모 개정입니다. 내부감사의 정의, 윤리규범, 표준 등의 변경은 없는 반면, 내부감사의 새로운 미션과 업무수행의 핵심원칙을 제시한 것이 두드러진 특징입니다. "리스크에 기반한 객관적인 확신과 자문의 제공을 통해 기업의 가치를 확대하고 보호하는" 내부감사의 미션은, 내부감사가 달성하기 위해 노력하여야 할 기준에 대한 기대수준을 높였습니다. IPPF 는 지배구조 속에서 내부감사의 역할과 핵심 이해관계자들에게 자문을 제공할 필요성을 언급하고 있습니다. 그럼에도 불구하고, 여전히 많은 내부감사조직들이 기존에 잘 갖추어진 통제나 SOX 등 기본적인 것에 관한 확신을 제공하는데 큰 비중을 두고 있습니다.

Steps to consider:

IPPF 에서 언급한 미션을 충족하기 위해 현재 내부감사의 업무방식을 평가하고 필요한 변화를 파악해야 합니다.

- 내부감사가 미션과 핵심 원칙을 얼마나 충족하고 있는지를 검토
- 내부감사 품질평가 프로그램이 존재하는지, 내부감사 품질은 어떻게 측정되는지를 검토
- 내부감사계획 중 "확신 제공"과 "자문" 기능 각각에 투입된 비율을 검토
- IPPF 를 내부감사가 창출해야 할 가치에 대비한 현재의 활동을 평가하는 논의의 출발점을 활용 (이는 과거의 관습에 젖어 있는 경영진과 이사회를 교육하는 수단으로도 활용 가능)
- IIA 가이드라인의 변경을 모니터링하고, 내부평가, 외부평가 혹은 독립적인 검증으로 보완하는 자가평가를 통해 내부감사의 운영실태를 IIA 기준과 비교

.