IT 감사 프레임워크(ITAF™)

IT 감사 전문가 실무수행 프레임워크

제4판

ISACA®

ISACA 소개

50년 넘게 ISACA®(*www.isaca.org*)는 기술에서 최고의 인재, 전문 지식 및 교육을 발전시켜 왔습니다. ISACA는 개인이 자신의 경력을 발전시켜 나가고 조직의 변혁을 도모할 수 있는 지식, 자격증명, 교육 및 커뮤니티를 갖출 수 있게 하고, 기업이 양질의 팀을 양성하고 구축할 수 있게 합니다. ISACA는 기술을 통한 혁신을 추진하는 정보보안, 거버넌스, 보증, 위험 및 개인정보 보호 분야에 종사하는 14만5천 명의 회원들이 가지고 있는 전문 지식을 활용하는 세계적인 전문가 협회이자 학습 단체입니다. ISACA는 전 세계 188개국에 220여 개의 지부가 있습니다.

면책사항

ISACA는 자체 *IT 감사 프레임워크(ITAF™): IT 감사 전문가 실무수행 프레임워크, 제4판*("저작물")을 기본적으로 보증 실무자들을 위한 교육 자원으로 설계하고 작성했습니다. ISACA의 저작물을 사용한다고 해서 항상 성공적인 결과를 가지고 오는 것은 아닙니다. 본 저작물이 적합한 정보와 절차 및 테스트를 모두 포함하고 있거나, 합리적으로 동일한 결과를 가져올 수 있는 다른 정보와 절차 및 테스트를 배제한 것으로 간주되어서는 안 됩니다. 어떤 정보, 절차 또는 테스트가 적합한지 판단하는 데 있어서, 보증 실무자는 자신의 전문적 판단을 특정 시스템이나 정보기술(IT) 환경에 있는 특수한 환경에 적용해야 합니다.

ISACA
1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
전화: +1.847.660.5505
팩스: +1.847.253.1755
문의처: https://support.isaca.org
웹사이트: www.isaca.org

피드백 제공: https://support.isaca.org
ISACA 온라인 포럼 참여: https://engage.isaca.org/onlineforums

트위터: http://twitter.com/ISACANews
LinkedIn: www.linkedin.com/company/isaca
페이스북: www.facebook.com/ISACAGlobal
인스타그램: www.instagram.com/isacanews/

IT 감사 프레임워크(ITAF™): IT 감사 전문가 실무수행 프레임워크, 제4판
미국에서 인쇄

감사의 글

ISACA는 다음 사항을 인정합니다:

전문가 검수자

Manoj Agarwal, CISA, CIA, CRMA, CA, DISA, Metro Brands Limited, 인도
G.M. Faruk Ahmed, CISA, Rupali Bank Limited, 방글라데시
Winnie Ang, CISA, CISM, 싱가포르
Anagha Apte, CISA, CRISC, CISM, Birlasoft Ltd., 미국
Kenia Arias, CISA, A-FE Consulting LLC,미국
Bode Bary Aro, CISA, CRISC, Enugu Electricity Distribution Company, 나이지리아
Mais Barouqa, CISA, CRISC, CGEIT, ISO27K, ITIL, COBIT FL, GRCP, Deloitte, 요르단
Marquita Bass, CISA, PMP, Rausch Advisory, 미국
Cindy Baxter, CISA, ITIL, State Street Corporation, 미국
Zsolt Bederna, CISA, CRISC, CISM, CGEIT, CISSP, CEH, ITIL-F, Cyex OÜ, 헝가리
Vijay Bhalerao, CISA, COBIT-F, ISO 27001 LA, MCSA, ITIL-F, Unisoft Computrade Pvt. Ltd., 인도
Parmeet Bhatiya, CISA, PricewaterhouseCoopers, 아랍 에미리트
Bakan Borupile, CISA, MCSE, MCSA, Btech, Mascom Wireless, 보츠와나
Ricardo Jimenez Caicedo, CISA, Ernst & Young, 콜롬비아
Jules Chachine, CISA, CISM, PMP, Jconseil, 레바논
Elastos Chimwanda, CISA, CIA, ZWMB Bank Limited, 짐바브웨
Joyce Chua, CISA, CISM, CDPSE, CIPP(E), (C)CISO, CIPM, CIPP(A), CFE, CIA, PMP, CITPM, ITIL, MCP, IRCA ISMS Associate Auditor, Sony Electronics, 싱가포르
Ari Ecrument, CISA, CRISC, CDPSE, FIP, CIPP/E, CIPM, CRMA, CEH, ISO 27001/22301/20000
Bhaskar Ghosh, CISA, Wintrust Financial Corporation, 미국
Miguel A. Gonzalez, CISA, ITESM, 멕시코
J. Winston Hayden, CISA, CRISC, CISM, CGEIT, 남아프리카
Andrew Hinder, CISA, CMIIA, QIAL, CRMA, CIA, BAE Systems, 영국
Marko Jagodic, CISA, CRISC, VRIS, LLC, 슬로베니아
Ashane J.W. Jayasekara, CISA, BDO, 스리랑카
Daniel Jones, CISA, CRISC, CISM, Devon Energy, 미국
Abbie Anne Julien, CISA, CDPSE, Life Extension Foundation Buyers Club Inc., 미국
Mladen Kandic, CISA, CIA, Eurobank, 세르비아
Joanna Karczewska, CISA, 폴란드
Glenn Kirke, CISA, 통합 감사 및 컴플라이언스, 미국
Matthias Kraft, CISA, CRISC, CISM, CGEIT, CAC, DPO, Fidelity International, 룩셈부르크
Abhishek Kumar, CISA, ISO 27001 LA, ISO 22301 LA, Deloitte, 인도
Hiu Sing Lam, CISA, FRM, PMP, 홍콩
James Lam, CISA, CRISC, CISM, TOGAF, Aon Cybersecurity Advisory, 미국
Larry L. Lliran, CISA, CISM, Precelsus Consulting, 푸에르토리코
Angel Giovanni Vasquez Lopez, CISA, Banco GYT Continental, 과테말라
Michael Malcolm, CISA, CIA, CRMA, CFSA, CGAP, CFE, Opentext Corporation, 캐나다
A.T. Manjunath, CISA, CCSK, CSA STAR AUDITOR, Applied Materials, 인도
Rafael Pérez Marín, CISA, 베네수엘라
Larry Marks, CISA, CRISC, CISM, CGEIT, CDPSE, CISSP, ITIL, PMP, 미국
Vivek Mathivanan, CISA, CRISC, CGEIT, Worley, 호주
Benedicta Mlingi, CISA, NMB Bank Plc., 탄자니아
Juan Carlos Morales, CISA, CRISC, CISM, CGEIT, COBIT 2019, 과테말라
Donald Morgan, CISA, Farm Credit Canada, 캐나다
Syed Aun Muhammad, CISA, 캐나다

감사의 글 *(계속)*

Christine Lilian Mukhongo, CISA, CRISC, CISM, KUCCPS(Kenya Universities & Colleges Central Placement Service), 케냐
Sitambaram Ainslei Naidu, CISA, CIA, Edcon, 남아프리카
Tushar Nerurkar, CISA, CISSP, PMP, PricewaterhouseCoopers 미국
Daisha Ngo, CISA, CPA, CRMA, Spectrum Health, 미국
Geoffrey Nkuutu, CISA, Fellow Chartered Certified Accountant (FCCA), Wazalendo Savings & Credit Cooperative Society Limited, 우간다
Alexander Obraztsov, CISA, CISSP, PMP, Societe Generale(뉴욕), 미국
Darren O'Brien, CISA, CRISC, Vitality, 영국
Iroko Oluwatosin, CISA, CRISC, CISM, ITIL, CEH, ISO 27001, Alberta Blue Cross, 캐나다
Anas Olateju Oyewole, CISA, CRISC, CISM, CDPSE, CISO, CISSP, CCSP, PMP, Indigo Books and Music, 캐나다
Chirag Ali Peerzada, CISA, CEH, ISO 27001 LA, ISO 22301 LI, Mahindra Special Service Group, 인도
John Pouey, CISA, CRISC, CISM, CIA, Entergy, 미국
Shahid Qureshi, CISA, CPA, CGA(캐나다), FCCA(영국), CIA(미국), FCMA, FCIS, FCSM, Leverage Global Inc., 캐나다
Sreechith Radhakrishnan, CISA, CRISC, CISM, CGEIT, CDPSE, COBIT Assessor, ISO 27001 LA, ISO 20000 LA, ISO 37001 LA, ISO 22301 LA, Global Success Systems FZ LLC, 아랍 에미리트
Allan Rono, CISA, CISM, ITIL, Liberty Group, 케냐
Sampa David Sampa, CISA, World Vision International, 잠비아
Megah Santio, CISA, CISM, COBIT Assessor, CIA, 호주
Garimella Chandrasekhar Sarma, CISA, CRISC, CDPSE, CFE, CtrlS Datacenters, 인도
S. Phani Krishna Sunkaranam, CISA, CRISC, CISM, CISSP, ITIL, Trianz, 인도
Luong Trung Thanh, CISA, CISM, CGEIT, 베트남
Catalin Tiganila, CISA, CRISC, CISM, CISSP, CBCP, CIPM, Deloitte, 룩셈부르크
Marisela Parra Valencia, CISA, ITIL, 코스타리카
Kaysi Veatch, CISA, CSX-F, CIA, Maxar, 미국
Ionnis Vittas, CISA, CISM, Quest Holdings SA, 그리스
Ross Wescott, CISA, CUERME, CCP, CIA (ret), Wescott & Associates, 미국
Surendra Yakkali, CISA, CSM, ITIL, SAFe 5, CMMI Associate, OptumServe Technology Services, Inc., 미국

이사회

Tracey Dedrick, 회장, 전 CRO(최고위험관리자), Hudson City Bancorp, 미국
Rolf von Roessing, 부회장, CISA, CISM, CGEIT, CDPSE, CISSP, FBCI, 파트너, FORFA Consulting AG, 스위스
Gabriela Hernandez-Cardoso, 독립 이사, 멕시코
Pam Nigro, CISA, CRISC, CGEIT, CRMA, 정보기술(IT)-부사장, 보안책임자, Home Access Health, 미국
Maureen O'Connell, 회장, Acacia Research(나스닥), 전 CFO(최고재무책임자) 겸 CAO(최고행정책임자), Scholastic, Inc., 미국
David Samuelson, CEO(최고경영자), ISACA, 미국
Gerrard Schmid, 사장 겸 CEO(최고경영자), Diebold Nixdorf, 미국
Gregory Touhill, CISM, CISSP, 사장, AppGate Federal Group, 미국
Asaf Weisberg, CISA, CRISC, CISM, CGEIT, CEO(최고경영자), introSight Ltd., 이스라엘
Anna Yip, CEO(최고경영자), SmarTone Telecommunications Limited, 홍콩
Brennan P. Baybeck, CISA, CRISC, CISM, CISSP, ISACA 회장, 2019-2020, 고객 서비스 부사장 겸 CISO(최고정보보호책임자), Oracle Corporation, 미국
Rob Clyde, CISM, ISACA 회장, 2018-2019, 독립 이사, Titus, 경영 회장, White Cloud Security, 미국
Chris K. Dimitriadis, Ph.D., CISA, CRISC, CISM, ISACA 회장, 2015-2017, 그룹 CEO(최고경영자), INTRALOT, 그리스

목 차

소개 7
자주 묻는 질문(FAQ) 7
조직 7
ITAF 사용 8
기타 표준 설정 기구에서 발행한 표준 9
용어 및 정의 9
ISACA 직업윤리강령 9
IT 감사 및 보증 표준양식 11
표준양식 11
일반 표준 11
수행 기준 12
보고 표준 15
일반 표준 17
일반 표준 1001: 감사 헌장 17
일반 지침 2001: 감사 헌장 17
일반 표준 1002: 조직의 독립성 20
일반 지침 2002: 조직의 독립성 20
일반 표준 1003: 감사자 객관성 22
일반 지침 2003: 감사자 객관성 22
일반 표준 1004: 합리적 기대 28
일반 지침 2004: 합리적 기대 28
일반 표준 1005: 정당한 주의의무 31
일반 지침 2005: 정당한 주의의무 31
일반 표준 1006: 숙련성 34
일반 지침 2006: 숙련성 34
일반 표준 1007: 의견 표명 37
일반 지침 2007: 의견 표명 38
일반 표준 1008: 기준 41
일반 지침 2008: 기준 41
수행 기준 45
수행 기준 1201: 계획 수립 시 위험 평가 45
수행 지침 2201: 계획 수립 시 위험 평가 45
수행 표준 1202: 감사 스케줄링 50
수행 지침 2202: 감사 스케줄링 50
수행 표준 1203: 업무 계획 51
수행 지침 2203: 업무 계획 52
수행 표준 1204: 수행 및 감독 57
수행 지침 2204: 수행 및 감독 57
수행 표준 1205: 증거 63
수행 지침 2205: 증거 63
수행 표준 1206: 외부 전문가의 활용 67
수행 지침 2206: 외부 전문가의 활용 68
수행 표준 1207: 부정 및 불법 행위 71
수행 지침 2207: 부정 및 불법 행위 71
보고 표준 81
보고 표준 1401: 보고 81
보고 지침 2401: 보고 81
보고 표준 1402: 사후 활동 84
보고 지침 2402: 사후 활동 84

부록 A: 관련 표준 및 표준별 지침 89
부록 B: 지침별 관련 표준.....91
부록 C: 용어 및 정의 93

소개

ISACA의 정보기술(IT) 감사 프레임워크(ITAF)는 다음 기능을 위한 종합적인 IT 감사 프레임워크입니다.

- IT 감사 및 보증 실무자의 역할과 책임, 윤리, 기대되는 전문가 행동 및 필요한 지식과 기술을 다루는 표준을 수립합니다.
- IT 감사 및 보증에 특정한 용어 및 개념을 정의합니다.
- IT 감사 및 보증 업무를 계획, 수행 및 보고하기 위한 지침과 기술을 제공합니다.

ISACA 자료에 기반한, ITAF는 IT 감사 및 보증 실무자들이 감사 수행 및 효과적인 감사 보고서 개발에 대한 안내를 얻기 위한 단일 소스를 제공합니다. ITAF의 제3판은 2013년 11월 1일부로 유효해진 IT 감사 및 보증 표준 및 지침을 통합했습니다. ITAF의 제4판을 발행하기 전, ISACA는 외부 의견을 위한 공개 초안을 발표했고 65명 이상의 검토자들이 피드백을 제공했습니다. ITAF의 제4판은 2020년 10월에 유효해집니다.

이러한 표준의 번역본은 *https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf4*에서 사용할 수 있습니다.

자주 묻는 질문(FAQ)

- **ITAF는 누구에게 적용됩니까?** ITAF는 IT 감사 및 보증 실무자의 역할을 수행하고 IT 프로세스, IT 애플리케이션의 구성요소, 시스템 및 인프라에 대한 보증을 제공하는 데 참여하는 개인에게 적용됩니다. 그러나, IT 감사 및 보증 보고서의 사용자를 포함하여, 더 폭넓은 대상자들에게 유익할 수 있는 방식으로도 이러한 표준, 지침 및 감사 기법을 설계하도록 주의를 기울였습니다.
- **ITAF는 언제 사용되어야 합니까?** 프레임워크의 애플리케이션은 IT 감사 및 보증 작업을 실시하기 위한 전제조건입니다. 표준은 필수사항입니다. 지침, 도구 및 기법은 보증 작업을 수행하는 데 임의 지원을 제공하도록 설계되었습니다.
- **ITAF IT 감사 및 보증 표준과 관련 지침은 어떤 상황에서 사용되어야 합니까?** ITAF의 설계는 IT 감사 및 보증 실무자들이 IT 중심 감사를 진행하는 일부터 재무, 컴플라이언스 또는 운영 감사에 기여하는 일에 이르기까지, 요건과 유형이 다른 임무를 맡고 있음을 인식합니다. ITAF는 IT 감사 또는 평가 업무에 적용될 수 있습니다.
- **ITAF가 상담 및 자문 작업의 요건을 해결합니까?** IT 감사 및 보증 실무자들은 감사 수행뿐만 아니라, 고용주를 위해 또는 고객사를 대신하여 비감사 업무도 수행할 수 있습니다. 일반적으로 이러한 상담 및 자문 업무에는 특정 영역의 검토가 포함됩니다. 업무 성격(특히 테스트 정도 및 업무 범위)을 포함하여 다양한 이유로 해서, IT 감사 및 보증 실무자는 보통 공식적인 감사 보고서를 발행하지 않습니다. 대신, 상담 및 자문 작업은 일반적으로 현재 수행 및 개선 제안사항에 대한 의견(의견서를 통해 표현될 수 있음)으로 결론내립니다.
- **ITAF의 제4판은 언제 사용할 수 있습니까?** 수정된 IT 감사 프레임워크는 2020년 10월 제공됩니다.

조직

ITAF 표준은 3개 카테고리로 분류됩니다.

- **일반 표준(1000 시리즈)**—IT 보증 전문가의 안내 원칙을 자세히 설명합니다. IT 감사 및 보증 실무자의 윤리, 독립성, 객관성 및 정당한 주의 의무뿐만 아니라, 지식, 역량 및 숙련도를 포함하여(이에 제한되지 않음) 이러한 원칙은 모든 업무에 적용됩니다.

- **수행 기준(1200 시리즈)**—기획, 감독, 범주 작업, 위험 평가, 중요성, 자원 배치, 감독, 업무 관리, 감사 및 보증 증거, 전문가적 판단 및 전문가적 정당한 주의 등 업무 수행을 다룹니다.
- **보고 표준(1400 시리즈)**—보고서 유형, 의사 소통 방식, 의사 소통된 정보를 다룹니다.

ITAF 지침은 IT 감사 및 보증 실무자에게 IT 감사 또는 보증 업무에 대한 정보와 방향성을 제공합니다. 위에서 개괄한 세 가지 표준 카테고리와 함께, 지침은 IT 프로세스, 통제 및 관련 IT 감사 또는 보증 과제를 계획하고, 실행, 평가, 테스트 및 보고하는 과정을 지원하는 다양한 감사 접근방식, 방법론 및 관련 자료에 중점을 둡니다. 또한 지침은 기업이 수행한 활동 및 계획과 IT에서 수행한 활동 및 계획 간의 관계를 명확히 하는 데 도움을 줍니다. 해당 지침은 관련 표준을 따릅니다.

ISACA의 웹사이트는 다양한 방법론, 도구 및 템플릿에 대한 구체적인 정보를 제공하고, 지침에서 정보를 사용하고 적용하는 데 방향성을 포함합니다. 예를 들어, ISACA의 수행 지침 2208(ITAF 프레임워크의 동반 지침인, 정보기술(IT) 감사 샘플링)이 작성되었습니다. 이 지침은 해당 모집단의 100% 미만으로 감사 절차를 적용할 때, 샘플링을 사용하여 전체 모집단에 대한 결론을 도출하는 것을 지원합니다. 백서, 감사 프로그램 및 책도 포함하는 추가 도구 및 기법은 *www.isaca.org/resources/insights-and-expertise/audit-program-and-tools*에서 사용할 수 있습니다.

ITAF 사용

IT 감사 및 보증 프로세스는 주제 사안에 대한 합리적 확신을 제공하는 특정 절차의 수행을 포함합니다. IT 감사 및 보증 실무자들은 검토에서 인증 또는 검사에 이르기까지 다양한 수준에서 보증을 제공하도록 설계된 업무를 수행합니다.

각 IT 감사 또는 보증 업무는 개인이 작업을 수행하기에 적격한지 여부, 작업이 수행되는 방식, 수행되는 작업, 그리고 업무의 다양한 특성과 획득된 결과의 성격에 기반하여 결과가 보고되는 방식에 있어서 규정된 표준을 준수해야 합니다.

한 사람이 업무를 수행할 경우, 그 사람은 업무를 완료하는 데 필요한 기술과 지식을 가지고 있어야만 합니다. 두 사람 이상이 업무를 수행할 경우, 해당 팀은 집합적으로 업무를 수행하기 위한 기술과 지식을 가져야 합니다.

IT 감사 또는 보증 업무에는 다음을 포함하여 여러 가지 중요한 추정사항이 내재되어 있습니다.

- 주제 문제(subject matter)는 식별될 수 있고 감사 대상입니다.
- 프로젝트의 성공적으로 완료될 확률이 높습니다.
- 접근방식과 방법론에서 편향이 없습니다.
- 프로젝트는 IT 감사 또는 보증 목적을 충족하기에 충분한 범위입니다.
- 프로젝트는 객관적이고 독자를 오도하지 않을 보고서로 이어집니다.

표준은 모든 경우에 필수적입니다. “shall” 용어는 “must(해야 함)”를 나타냅니다. 표준과의 편차는 IT 감사 또는 보증 업무를 완료하기 전에 해결되어야 합니다.

지침이 모든 상황에 적용될 수 있는 것은 아니지만, 항상 고려되어야 합니다. 지침은 IT 감사 및 보증 실무자들에게 일정 정도의 유연성을 허용합니다. 따라서 지침을 검토하여 적용가능성을 판별할 때, 실무자들은 전문가 판단을 사용하고, 지침과의 유의미한 차이나 지침의 관련 부분 생략을 정당화할 준비를 하고, 필요한 경우 추가 지침을 구해야 합니다.

추가 지침을 위한 자원으로 다음을 포함할 수 있습니다.

- 기업 내부 및/또는 외부 동료(예: 전문가 협회 또는 전문가 네트워크 그룹을 통해)
- 경영진
- 기업의 지배기구(예: 감사 위원회)
- 전문적 지침 자료(예: 책, 논문, 기타 지침)

도구 및 기법은 안내를 지원하는 보충 자료 및 정보를 나타냅니다. 일부 경우, 기법은 대체 또는 다양한 기법을 나타낼 수 있으며, 이들 중 많은 기법이 적용될 수 있습니다. IT 감사 및 보증 실무자는 관련성이 있고 객관적이며 편향적이지 않은 정보를 생성하는 적합한 기법만 선택해야 합니다.

ITAF의 지속적인 발전과 함께, 섹션 번호는 의도적으로 향후 지침의 추가를 위한 공백을 포함합니다.

기타 표준 설정 기구에서 발행한 표준

ITAF 표준은 IT 감사 및 보증 실무자들에게 포괄적인 지침과 방향성을 제공하면서, 일부 상황에서는 실무자들이 다른 조직에서 발행한 표준을 사용해야 할 수 있습니다.

IT 감사 및 보증 실무자가 ITAF 표준 준수를 인용했을 때, ITAF와 다른 조직의 해당 표준 간에 충돌이 발생하면 IT 감사 및 보증 실무자는 검토를 실시하고 결과를 보고하기 위한 일반적인 표준으로서 ITAF표준을 사용해야 합니다.

IT 감사 및 보증 실무자가 규제 목적이나 운영상의 기대치를 위해 ITAF 이외의 표준을 준수해야 하는 경우, IT 감사 및 보증 실무자는 다음을 수행할 수 있습니다.

- ITAF 표준과 함께 기타 권위있는 기관에서 요구하는 전문가 표준을 사용합니다.
- 보고서에서 기타 필요한 표준 사용을 인용합니다.

용어 및 정의

본 문서 전반에 걸쳐서, 공통 단어는 IT 감사 및 보증 실무자들이 수행한 업무 중 가장 공통적인 유형에 적용되는 특정한 의미로 사용됩니다. 이러한 예에서 정의는 ITAF에 대한 부록 C에 제공되어 있습니다. 이것은 본 문서의 문맥 내에서 단어와 그 의미가 이해되고 일관되게 적용되도록 합니다.

실용적인 상황에서 ITAF 용어 및 정의는 일반적으로 전문가의 감사 수행과 정보 기술 및 보안에서 공통적으로 사용되는 용어와 일치하지만, 실무자들은 수행될 특정 유형의 계약과 관련된 가장 최신의 원본 표준을 참조하여 가장 최신의 적합한 용어와 정의가 사용되도록 합니다.

ITAF에 포함되지 않은 기타 용어 및 정의는 ISACA 웹사이트, *www.isaca.org/glossary*에서 전체 용어집을 사용할 수 있습니다.

ISACA 직업윤리강령

ISACA는 아래와 같은 직업윤리강령(Code of Professional Ethics)을 통해 협회 회원 및 자격증 소지자의 직업적이고 개인적인 행위에 대한 지침을 제시합니다.

회원과 ISACA 자격증 소지자는 다음과 같은 규정을 준수해야 합니다.

1. 기업 정보 시스템 및 기술의 효과적인 거버넌스 및 관리(감사, 통제, 보안 및 위험 관리)를 위한 적절한 표준 및 절차 이행을 지원하고 준수를 독려합니다.
2. 직업 표준에 따라 객관적으로 정당한 주의의무를 가지고 전문적인 방식으로 임무를 수행해야 합니다.
3. 높은 수준의 행위와 품격을 유지하면서 합법적인 방식으로 관련 당사자의 이익을 위해 일하고, 해당 직업 또는 협회의 신뢰를 떨어뜨리지 않아야 합니다.
4. 사법 당국에 의해 공개가 요구되지 않는 한 활동 과정에서 습득한 정보의 프라이버시와 기밀을 유지해야 합니다. 이러한 정보는 개인적인 목적으로 사용하거나 부적절한 대상에게 공개할 수 없습니다.
5. 해당 분야에서 역량을 유지하고 필요한 기술, 지식 및 역량으로 완료할 수 있을 것으로 합리적으로 예상되는 활동만을 수행하는데 동의해야 합니다.
6. 관련자에게 알려진 모든 중요 사실의 공개를 포함하여, 수행된 작업의 결과를 관련자에게 알립니다. 만약 공개하지 않으면 결과 보고가 왜곡될 수 있습니다.
7. 기업 정보 시스템 및 기술의 거버넌스 및 관리(감사, 통제, 보안 및 위험 관리)에 대한 이해를 높이기 위한 이해관계자들의 전문가 교육을 지원합니다.

이러한 직업윤리강령(Code of Professional Ethics)을 준수하지 못할 경우 회원 또는 자격증 소지자의 행위에 대한 조사에 이어 궁극적으로 징계 조치가 취해질 수 있습니다.

IT 감사 및 보증 표준양식

ITAF의 표준은 IT 감사 및 보증 실무자를 지원하기 위해 설계된 주요 양상을 포함합니다. ITAF 표준은 주기적으로 검토되어 지속적으로 개선되고 IT 감사 및 보증 직업의 발전과 보조를 맞추기 위해 필요에 따라 수정됩니다.

표준양식

일반 표준

1001 감사 헌장

1001.1 IT 감사 및 보증 담당자는 감사 헌장에 감사 기능을 적합하게 문서화하고 목적, 책임, 권한 및 책임추적성을 명시해야 합니다.

1001.2 IT 감사 및 보증 담당자는 감사 헌장이 감사 담당자의 거버넌스 및 감독 책임자들(예: 이사회 및/또는 감사 위원회)에 의해 합의되고 공식적으로 승인되도록 해야 합니다.

1001.3 IT 감사 및 보증 담당자는 감사 헌장을 경영진/고위 관리지에 전달해야 합니다. 또한 감사 헌장의 관련 요소를 착수 회의에서 및/또는 계약서를 통해 감사 받는 그룹과 공유해야 합니다.

1001.4 주기적으로 감사 헌장을 검토하여, 감사 및 보증 담당자의 책임은 감사 헌장에 반영된 대로, 기업의 미션 및 전략에 맞추어 유지되어야 합니다. 기업의 미션 또는 전략이 변경될 경우 또는 감사 담당자의 책임이 변경될 경우에는 즉각적인 감사 헌장의 검토가 보증되어야 합니다.

1002 조직의 독립성

1002.1 IT 감사 및 보증 담당자는 감사 및 보증 업무와 관련된 모든 문제에서 이해 충돌 및 과도한 영향이 없어야 합니다. (실제로 또는 겉으로 보기에) 모든 독립성의 훼손은 식별되고 해당 당사자에게 공개됩니다.

1002.2 IT 감사 및 보증 담당자는 과도한 영향으로부터 자유로울 수 있는 기능의 능력을 지원하는 기능 보고 관계(예: 이사회에 보고함)를 가져야 합니다.

1002.3 IT 감사 및 보증 담당자는 담당자가 아무런 방해 없이 그 책임을 수행할 수 있도록 지원하는 관리 보고 관계(예: 업무, 현장 작업 또는 보고 범위)를 가져야 합니다.

1003 감사자 객관성

1003.1 IT 감사 및 보증 실무자는 감사 및 보증 업무와 관련된 모든 문제에서 객관적이어야 합니다.

1004 합리적 기대

1004.1 IT 감사 및 보증 실무자는 해당 IT 감사 및 보증 표준과 필요 시 기타 산업 표준 또는 해당 법과 규정에 의거하여 업무를 완료하여 전문가 의견이나 결론을 도출할 수 있다는 합리적인 기대를 가져야 합니다.

1004.2 IT 감사 및 보증 실무자는 업무의 범위를 통해 해당 주제에 대한 결론을 낼 수 있고, 범위 제한이 지정된다는 합리적인 기대를 가져야 합니다.

1004.3 IT 감사 및 보증 실무자는 관리진이 업무를 수행하는 데 필요한 적절하고 관련성 있고 시기 적절한 정보를 제공하는 것과 관련하여 의무와 책임을 이해한다는 합리적인 기대를 가져야 합니다.

1005 정당한 주의의무

1005.1 ISACA의 직업윤리강령에 따라, 감사자들은 주의의무를 가지고 전문적인 방식으로 임무를 수행합니다. 이들은 높은 수준의 행동과 인격을 유지할 것이며, 그들 자신이나 직업의 신뢰를 훼손시킬 수 있는 행위에 관여하지 않도록 합니다. 감사자의 임무 수행 과정에서 얻은 정보의 개인정보 보호 및 기밀성을 유지해야 합니다. 뿐만 아니라, 이 정보는 개인의 이익에 사용하거나 법적 기관에서 요구하는 경우가 아니면 공개해선 안됩니다.

1006 숙련성

1006.1 감사 및 보증 업무 보조자와 총칭해서, IT 감사 및 보증 실무자는 필요한 작업을 수행할 수 있는 전문적 역량을 갖추어야 합니다.

1006.2 IT감사 및 보증 실무자들은 IT 감사 및 보증 업무에서 자신들의 역할을 수행하기 위해 해당 주제에 대한 적절한 지식을 가지고 있어야 합니다.

1006.3 IT 감사 및 보증 실무자는 지속적으로 적절한 직무 교육과 훈련을 통하여 전문직 종사자로서 전문성을 유지해야 합니다.

1007 의견 표명

1007.1 IT 감사 및 보증 실무자는 감사 주제가 평가될 때 기준이 되는 의견 표명을 검토하여, 해당 의견 표명이 감사 대상 자질이 있는지 및 의견 표명이 충분하고, 유효하며, 적절한지를 파악해야 합니다.

1008 판단기준

1008.1 IT 감사 및 보증 실무자는 주제 사안이 평가될 때 바탕이 되는 객관적이고, 온전하며, 적절하고, 측정 가능하고, 이해 가능하며, 널리 인식되고, 권한이 있고, 보고서의 모든 독자 및 사용자가 이해할 수 있고 이들이 이용할 수 있는 판단기준을 선택해야 합니다.

1008.2 IT 감사 및 보증 실무자는 판단기준의 수용 가능성을 고려하여야 하며, 인정되고 권위가 있으며 공개적으로 사용할 수 있는 기준에 중점을 두어야 합니다.

수행 기준

1201 계획 수립 시 위험 평가

1201.1 IT 감사 및 보증 담당자는 적절한 위험 평가 접근 방식(즉, 수량적 및 정성적 요인을 모두 포함한 데이터 중심)과 제반 방법을 사용하여 전반적인 IT 감사 계획서를 수립하고 IT 감사 자원의 효과적 할당을 위한 우선순위를 결정해야 합니다.

1201.2 IT 감사 및 보증 실무자는 개별 업무를 계획할 때 검토 대상 영역과 관련된 위험을 식별하고 평가해야 합니다.

1201.3 IT 감사 및 보증 실무자는 감사 업무를 계획할 때 해당 주제에 대한 지식, 감사 위험 및 기업에 대한 관련 노출을 고려해야 합니다.

1202 감사 일정

1202.1 IT 감사 및 보증 담당자는 단기 및 장기간 감사 일정을 만드는 전체 전략적 계획을 세워야 합니다. 단기간 계획은 연내에 수행될 감사로 구성되는 반면, 장기간 계획은 미래에 수행될 수 있는 기업의 정보 및 기술(I&T) 환경 내 위험 관련 문제에 기반한 감사로 구성됩니다.

1202.2 단기간 및 장기간 감사 일정은 모두 거버넌스 및 감독 책임자(예: 감사 위원회)와 합의해야 하고 기업 내에서 소통되어야 합니다.

1202.3 IT 감사 및 보증 담당자는 조직의 필요(즉, 예기치 않은 이벤트 또는 예정되지 않은 신규 계획)에 대응하도록 단기간 및/또는 장기간 감사 일정을 수정해야 합니다. 예기치 않은 이벤트 또는 예정되지 않은 신규 계획의 감사를 수용하도록 대체된 감사는 추후 다시 할당되어야 합니다.

1203 업무 계획

1203.1 IT 감사 및 보증 실무자는 수행할 감사 절차의 성격, 타이밍 및 범위를 다루는 각 IT 감사 및 보증 업무를 계획해야 합니다. 계획은 다음 사항을 포함해야 합니다.

- 감사 대상 영역
- 목적
- 범위
- 자원(예: 실무진, 도구 및 예산) 및 일정 날짜
- 시간표 및 납품
- 준거법/규정 및 전문 감사 표준 준수
- 법적 또는 규정 준수와 관련되지 않은 업무에 대한 위험 기반 접근방식 사용
- 업무별 이슈
- 문서화 및 보고 요건
- 관련 기술 및 데이터 분석법 사용
- 잠재적 이익에 대한 업무 비용 고려
- IT 감사 업무 수행 중 발생할 수 있는 상황에 대한 알림 및 단계적 확대 프로토콜(예: 핵심 인력의 범위 제한 또는 사용 불가능)

현장 작업 중, 업무 진행에 따라 계획 중 생성된 감사 절차를 수정해야 할 수 있습니다.

1203.2 IT 감사 및 보증 실무자는 감사를 완료하는 데 사용될 단계별 절차와 지침을 설명하는IT 감사 및 보증 업무 감사 프로그램을 개발하고 문서화해야 합니다.

1204 수행 및 감독

1204.1 IT 감사 및 보증 실무자는 승인된 IT 감사 계획에 따라 작업을 수행하여 합의된 일정 내에서 식별된 위험을 처리해야 합니다.

1204.2 IT 감사 및 보증 실무자는 감독 책임이 있는 IT 감사 직원들을 감독하여 감사 목표를 달성하고 해당되는 전문 감사 표준을 충족해야 합니다.

1204.3 IT 감사 및 보증 실무자는 자신의 지식 및 기술 내에 있는 작업 또는 업무 중에 기술을 습득하거나감독 하에서 작업을 달성한다는 합리적인 기대가 있는 작업만을 수락해야 합니다.

1204.4 IT 감사 및 보증 실무자는 감사 목적을 달성하기 위한 충분하고 적절한 증거를 확보하고 보존해야 합니다.

1204.5 IT 감사 및 보증 실무자는 감사 과정을 문서화하고 감사 작업과 결과 및 결론을 지원하는 감사 증거를 기술해야 합니다.

1204.6 IT 감사 및 보증 실무자의 결과와 결론은 이 증거의 근본 원인 분석과 해석에 의해 지지되어야 합니다.

1204.7 IT 감사 및 보증 실무자는 적절한 감사 의견 또는 결론을 제공하고 필요한 증거가 추가 테스트 절차를 통해 획득되는 범위 제약 사항을 포함해야 합니다.

1205 증거

1205.1 IT 감사 및 보증 실무자는 납득할 만한 결론을 도출해내기 위한 충분하고 적절한 증거를 확보해야 합니다.

1205.2 IT 감사 및 보증 실무자는 전문가적 의구심을 적용하여, 결론을 지지하고 참여 목표를 달성하기 위해 확보한 증거의 충분성을 평가해야 합니다.

1205.3 IT 감사 및 보증 실무자는 다른 작업 서류와 함께, 공식적으로 정의되고 승인된 보존 기간과 일치하는 기간 동안 증거를 보존해야 합니다.

1206 다른 전문가의 작업 사용

1206.1 IT 감사 및 보증 실무자는 해당될 경우 업무를 위해 다른 전문가의 작업을 사용하는 것을 고려해야 합니다.

1206.2 IT 감사 및 보증 실무자는 업무 전에 다른 전문가의 전문 자격, 역량, 관련 경험, 자원, 독립성 및 품질 관리 프로세스의 타당성을 평가하고 승인해야 합니다.

1206.3 IT 감사 및 보증 실무자는 업무의 일환으로서 다른 전문가의 작업을 심사, 검토, 평가하고, 이 업무의 사용 및 의존 정도에 대한 결론을 문서화해야 합니다.

1206.4 IT 감사 및 보증 실무자는 업무 팀에 속하지 않은 다른 전문가의 작업이 적절하고 온전한지 여부를 결정해야 하여, 현재 업무 목표에 대해 결론을 내려야 합니다. 또한 실무자는 결론을 명확하게 문서화해야 합니다.

1206.5 IT 감사 및 보증 실무자는 다른 전문가의 업무가 보고서에 종속되어 직접 통합될지 또는 별도로 언급할지 여부를 결정해야 합니다.

1206.6 IT 감사 및 보증 실무자는 다른 전문가가 충분하고 적절한 증거를 제공하지 못하는 경우에 충분하고 적절한 증거를 얻을 수 있는 추가 테스트 절차를 적용해야 합니다.

1206.7 IT 감사 및 보증 실무자는 감사 의견 또는 결론을 제공하고 필요한 증거가 추가 테스트 절차를 통해 획득되지 않는 범위 제약 사항을 포함해야 합니다.

1207 부정 및 불법 행위

1207.1 IT 감사 및 보증 실무자는 업무 중 부정 및 불법 행위의 위험을 고려해야 합니다.

1207.2 IT 감사 및 보증 감사 실무자는 부정 또는 불법 행위를 문서화하고 관련 담당자에게 적시에 전달해야 합니다. 일부 커뮤니케이션(예: 규제자와)은 제한될 수 있습니다. 따라서, 실무자가 커뮤니케이션할 때 감사 기능의 거버넌스 및 감독 책임자(예: 이사회 및/또는 감사 위원회)와 논의해야 할 수 있습니다.

보고 표준

1401 보고

1401.1 IT 감사 및 보증 실무자는 각 업무의 결과를 전달하기 위한 보고서를 제공해야 합니다.

1401.2 IT 감사 및 보증 실무자는 감사보고서의 결과물이 충분하고 적합한 증거에 의해 뒷받침되도록 해야 합니다.

1402 사후 활동

1402.1 IT 감사 및 보증 실무자는 감사 기능(예: 이사회 및/또는 감사 위원회) 책임자에게 관리진의 결과 및 권장사항에 대한 진행상황을 정기적으로 보고해야 합니다. 보고는 경영진이 보고된 감사 결과와 권장사항을 다루기 위해 적시에 적절한 조치를 계획하고 취했는지 여부에 대한 결론을 포함해야 합니다.

1402.2 감사 결과 이행에 대한 전체 진행 상황은 감사 위원회가 제대로 있을 경우,감사 위원회에 정기적으로 보고해야 합니다.

1402.3 결과와 관련된 위험이 수용되었고 기업의 위험 수용범위보다 크다고 판단될 경우, 이 위험 수용은 고위 경영진과 논의해야 합니다. 위험(특히 위험 해결 실패)의 수용은 감사 위원회(제대로 있는 경우) 및/또는 이사회의 주목을 받아야 합니다.

이 페이지는 의도적으로 비워둠

일반 표준

일반 표준 1001: 감사 헌장

내용	**1001.1** IT 감사 및 보증 담당자는 감사 헌장에 감사 기능을 적합하게 문서화하고 목적, 책임, 권한 및 책임 추적성을 명시해야 합니다.
	1001.2 IT 감사 및 보증 담당자는 감사 헌장이 감사 담당자의 거버넌스 및 감독 책임자들(예: 이사회 및/또는 감사 위원회)에 의해 합의되고 공식적으로 승인되도록 해야 합니다.
	1001.3 IT 감사 및 보증 담당자는 감사 헌장을 경영진/고위 관리자에 전달해야 합니다. 또한 감사 헌장의 관련 요소를 착수 회의에서 및/또는 계약서를 통해 감사 받는 그룹과 공유해야 합니다.
	1001.4 주기적으로 감사 헌장을 검토하여, 감사 및 보증 담당자의 책임은 감사 헌장에 반영된 대로, 기업의 미션 및 전략에 맞추어 유지되어야 합니다. 기업의 미션 또는 전략이 변경될 경우 또는 감사 담당자의 책임이 변경될 경우에는 즉각적인 감사 헌장의 검토가 보증되어야 합니다.

일반 지침 2001: 감사 헌장

2001.1 실무자는 감사 기능을 수행하기 위한 명확한 권한을 가져야 합니다. 일반적으로 이러한 권한은 거버넌스 책임자(예: 이사회 및/또는 감사 위원회)가 공식적으로 승인해야 하는 감사 헌장에 문서화되어야 합니다. 감사 기능 전반에 대한 감사 헌장이 있으면, IT 감사 및 보증 권한이 통합되어야 합니다.

2001.2 감사 헌장 내용

2001.2.1	감사 헌장은 IT 감사 및 보증 기능을 문서화합니다. • 독립성, 윤리강령 및 표준 • 목적, 책임, 권한 및 책임 추적성 • 전달 및 단계적 확대를 포함하여(이에 제한되지 않음), IT 감사 및 보증 실무자는 업무의 수행에서 따르는 프로토콜 • IT 감사 또는 보증 업무 중 피감인의 역할 및 책임 • 부정 및 불법 행위 보고에서 IT 감사 및 보증 담당자의 역할
2001.2.2	감사 헌장은 감사 담당자의 목적, 책임, 권한 및 책임 추적성을 명확히 다루어야 합니다(2001.2.1 참조). 이러한 네 가지 측면이 다음 섹션에서 설명되어 있습니다.
2001.2.3	감사 담당자의 **목적**은 관리진이 구현한 통제 기능의 설계와 실행을 평가하고 테스트하는 것입니다. 감사 헌장은 그 목적을 달성하는 있어서 감사 담당자를 지원하는 다음 섹션을 포함해야 합니다. • **감사 담당자의 목적/목표**는 감사 담당자가 운영하는 기능 및 조직의 프레임워크를 제공합니다. • **감사 담당자 및 감사 담당자 임무 내용의 목적**(감사 담당자가 가지고 있는 경우)은 정보 시스템의 위험 관리 프로세스, 내부 통제 시스템 및 운영/거버넌스의 설계 및 운영 효과성을 평가하고 개선하기 위한 구조적 접근방식을 가져오는 것입니다. • **감사 담당자의 범위**는 전체 기업 또는 기업 내 특정 조직에 적용됩니다. • **감사 담당자가 수행하**는 작업은 정보 시스템 감사, 적합성 감사, 재정 감사, 운영 감사, 통합 감사, 행정 감사, 특별 감사(타사 서비스 감사, 사기 감사 또는 포렌식 감사), 컴퓨터 포렌식 감사 및 기능 감사를 포함할 수 있습니다. 또한 이것은 프로젝트의 컨설팅 서비스와 같은 비감사 서비스를 포함할 수 있습니다.

2001.2.4	감사 담당자의 **책임**은 기업에 가치를 더하여, 전략, 임무 및 규제/준수 기대와 같은 조직의 시각이 조직의 작업에 통합되고 전문가 기대(예: 윤리, 전문가 개발)에 부응하도록 하는 것입니다. 감사 헌장은 감사 담당자를 수월하게 하는 다음 섹션을 포함해야 합니다.
	• **독립성**은 표준 1002 조직 독립성 및 1003 감사자 객관성에 설명된 대로, 감사 담당자 및 실무자에 대한 독립성 요건 이행을 자세히 설명합니다. IT 감사 및 보증 담당자는 다음과 같은 방식으로 독립성을 보장해야 합니다.
	  ▪ 주기적으로(적어도 매년) 독립성을 평가함
	  ▪ 잠재적인 독립성 훼손의 식별 및 보고와 관련된 공식 프로토콜 생성 및 유지보수
	독립성 평가 및 훼손 프로토콜의 결과는 감사 담당자의 거버넌스 및 감독 책임자(예: 이사회 및/또는 감사위원회)에게 보고해야 합니다.
	• **외부 감사 회사와의 관계**는 내부 IT 감사 및 보증 담당자의 외부 감사자와 의존 전략을 자세히 기술합니다.
	  ▪ 외부 감사자와 회의하여 작업 중복을 최소화하기 위한 작업 업무를 조정함
	  ▪ 실무자의 작업 서류, 문서화 및 증거에 대한 액세스 제공
	  ▪ 예정 기간에 대한 감사 계획 초안을 작성할 때 외부 감사자들이 계획한 작업을 고려함
	• **피감인의 기대**는 피감인이 감사 담당자 및 실무자에게서 기대할 수 있는 서비스 및 산출물을 자세히 기술합니다.
	  ▪ 피감인의 책임 영역과 관련된 식별된 문제, 결과 및 가능한 해결책에 대한 설명
	  ▪ 감사 보고서의 결과에 대해 취하는 경영진 대응 및 시정조치 포함 가능성. 이것은 보고서 제공, 피감인 불만에 대한 대응, 서비스 품질, 수행 검토, 보고 프로세스 및 결과 동의와 같은 항목에 대한 관련 서비스 수준 계약(SLAs)의 참조를 포함합니다.
	• **피감인 요건**은 피감인의 책임을 자세히 기술합니다. 예를 들어, 모든 피감인은 스스로 이용할 수 있게 하고 감사 담당자 및 실무자가 할당된 책임을 이행하는 데 도움을 주어야 합니다. 또한 피감인 요건은 경영진의 책임 및 감사 담당자의 책임에 관하여 명확성을 제공합니다.
	• 감사자의 조직 및 감사자가 회원 자격을 가지는 표준 설정 기구에서 설정한 **전문가 표준을 준수**합니다.
	• 감사 담당자 및 실무자가 준수할 요건을 자세히 기술하는 표준 **준수**. 예를 들어, 감사 담당자 및 실무자는 모든 ISACA ITAF 감사 및 보증 표준 및 지침을 따르고 행동합니다.

2001.2.5	감사 담당자의 **권한**은 다음 섹션을 포함해야 합니다. ● 감사 업무를 수행하는 실무자의 관련 정보, 시스템(시스템에 구축된 로그, 활동 및 통제), 인력 및 위치에 대한 **액세스 권리**. IT 감사 실무자로 표현되는 감사 담당자: ■ 감사 업무를 수행하는데 필요한 임의 및 모든 레코드, 문서, 시스템 및 위치에 대한 접근 권한을 가지고 있으며, 이러한 접근 권한을 얻기 위해 경영진에게 도움을 요청할 수 있습니다. ■ 감사 업무를 수행할 때 직원, 컨설턴트 또는 계약업체로부터 정보를 얻을 수 있는 권한을 가집니다. ● 감사 담당자 및 실무자의 **권한 제한** ● 감사 담당자가 감사 권한을 가지는 **감사될 프로세스**. 즉, 감사 담당자는 위험 기반 감사 계획에 기반하여 감사할 프로세스를 자유롭게 판별합니다.
2001.2.6	감사 및 보증 담당자의 **책임추적성**은 다음 사항을 포함하며, 이에 제한되지는 않습니다. ● 적합한 이해관계자 및 감사 및 보증 담당자의 거버넌스 및 감독 책임자(즉, 이사회 및/또는 감사 위원회)에 **서면 알림 배포**(예: 감사 보고서 및 비감사 업무 제안서) ● 감사 권장사항에 대응하여 취한 합의된 이행(정정 조치)에 대한 **관리진의 진행상황 모니터링 및 보고** ● 감사 및 보증 담당자의 거버넌스 및 감독 책임자(예: 이사회 및/또는 감사 위원회)에 **감사 및 보증 담당자의 수행 측정 보고**(예: 감사 계획 및 예산과 관련된 수행) ● 담당자의 독립성 및 잠재적 독립성 훼손과 감사 담당자의 목적, 책임, 권한 및 책임 추적성의 4가지 측면에 대해 **감사 및 보증 담당자의 거버넌스 및 감독 책임자(예: 이사회 및/또는 감사 위원회)에게 보고** ● 감사 기능과 관련된 피감인의 요구와 기대에 대한 이해를 확립하는 **품질 보증 프로세스**(예: 인터뷰, 고객 만족도 조사, 과제 수행 조사). 이러한 요구는 필요에 따라 서비스를 개선하거나 서비스 제공 또는 감사 헌장을 변경한다는 시각으로 감사 헌장에 대해 평가되어야 합니다. ● 다음을 포함하지만 이에 국한되지 않는 **감사 업무에 대한 인력 배치 규칙**: ■ 감사 헌장에 의존하여 비감사 서비스(예: 컨설팅 서비스) 수행에서 실무자의 관여와 광범위한 성격, 서비스의 시기 및 범위를 허용하여 독립성과 객관성이 훼손되지 않도록 합니다. 이것은 사례별로 각 비감사 서비스에 대한 특정 권한을 얻어야 하는 필요성을 제거하거나 최소화할 수 있습니다. ■ 실무자들이 독립성을 훼손하는 비감사 서비스를 수행한 영역의 감사 업무에 참여하려면 거쳐야 하는 최소 기간을 설정합니다. ■ 감사 담당자 및 실무자의 행동에 대한 조치를 합의합니다(예: 당사자 중 어느 한쪽이 책임을 이행하지 않을 경우 처벌). ■ 피감인과의 커뮤니케이션은 감사 담당자가 피감인과 커뮤니케이션할 빈도 및 커뮤니케이션 채널을 상세히 기술합니다.

표준 1001 및 지침 2001을 위한 COBIT® 2019 연결

COBIT 2019 관리 목표	목적
MEA02 내부 통제 시스템 관리	내부 통제 시스템의 적절성에 대한 주요 이해관계자들의 투명성을 확보하여 운영에 대한 신뢰, 기업 목표 달성에 대한 확신, 그리고 잔여 위험에 대한 적절한 이해를 제공합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

일반 표준 1002: 조직의 독립성

내용	**1002.1** IT 감사 및 보증 담당자는 감사 및 보증 업무와 관련된 모든 문제에서 이해 충돌 및 과도한 영향이 없어야 합니다. (실제로 또는 겉으로 보기에) 모든 독립성의 훼손은 식별되고 해당 당사자에게 공개됩니다.
	1002.2 IT 감사 및 보증 담당자는 과도한 영향으로부터 자유로울 수 있는 기능의 능력을 지원하는 기능 보고 관계(예: 이사회에 보고함)를 가져야 합니다.
	1002.3 IT 감사 및 보증 담당자는 담당자가 아무런 방해 없이 그 책임을 수행할 수 있도록 지원하는 관리 보고 관계(예: 업무, 현장 작업 또는 보고 범위)를 가져야 합니다.

일반 지침 2002: 조직의 독립성

2002.1 소개 지침의 내용 부문은 IT 감사 및 보증 담당자의 독립성에 대한 정보를 제공하도록 구조화되었습니다.

2002.2 기업에서 위치

2002.3 보고 수준

2002.4 독립성 평가

2002.2 기업에서 위치

2002.2.1	조직의 독립성을 실현하기 위해서는 감사 담당자가 기업에서 간섭 없이 책임을 수행할 수 있는 위치에 있어야 합니다. 다음과 같은 작업으로 이를 성취할 수 있습니다. ● 감사 위원회 헌장에서 감사 담당자를 운영 부서 외부의 독립적인 담당자 또는 부서로 설정합니다. 감사 담당자에게는 어떠한 운영 책임이나 활동을 맡겨선 안됩니다. ● 감사 담당자가 기업 내에서 조직의 독립성을 성취할 수 있게 하는 수준에 보고하도록 합니다. 운영 부서장에게 보고할 경우 조직의 독립성이 훼손될 수 있습니다.
2002.2.2	감사 담당자는 관리 책임을 가정해야 하는 IT 계획에서 비감사 역할을 수행해선 안됩니다. 이러한 역할은 미래의 독립성을 훼손시킬 수 있기 때문입니다. 감사 담당자의 독립성 및 책임추적성은 감사 헌장에서 다루어져야 합니다. 감사자가 직접 관리 책임을 가지는 영역에서 업무를 계획하거나 업무에 참여하도록 예정되어 있는 경우 감사 담당자의 독립성이 훼손될 수 있습니다. IT 감사 및 보증 담당자는 기업의 외부 감사 회사와 협력하여, 직접적 또는 간접적 관리를 구성하는 책임을 판별할 수 있습니다. 또한 이 두 그룹은 감사인의 직접 관리 책임 수행과 해당 영역의 업무 참여 간에 허용 가능한 시간을 식별할 수 있습니다.

2002.3 보고 수준

2002.3.1	감사 담당자는 완벽한 조직의 독립성을 가지고 행동할 수 있는 수준에 보고해야 합니다. 독립성은 감사 헌장에 정의되고 감사 담당자가 정기적으로, 적어도 매년 이사회 및 거버넌스 책임자에게 확인해야 합니다.
2002.3.2	감사 담당자의 조직적 독립성을 보장하기 위해서는 입력 및/또는 승인을 위해 다음 사항을 거버넌스 책임자들(예: 이사회)에게 보고해야 합니다. • 감사 자원 계획 및 예산 • 위험 기반 감사 계획 • 감사 담당자가 IT 감사 활동에 대해 수행한 수행 사후 조사 • 상당한 범위 또는 자원 제한에 대한 사후 조사
2002.3.3	감사 담당자의 조직적 독립성을 보장하기 위해서는 이사 및 경영진 모두의 명확한 지원이 필요합니다. 경영진의 지원은 조직의 모든 수준으로 전달하는 서면 알림을 포함할 수 있습니다.

2002.4 독립성 평가

2002.4.1	독립성은 감사 담당자에 의해 정기적으로 평가되고 감사 담당자의 거버넌스 및 감독을 책임지는 이들(예: 이사회 및/또는 감사 위원회)에게서 확인되어야 합니다. 이 평가는 적어도 연례적으로 수행해야 합니다. 평가는 다음과 같은 요인을 고려해야 합니다. • 개인 관계의 변화 • 금융 금리 • 이전 직무 할당과 책임뿐만 아니라 현재 직무 할당 역할과 책임에 대한 제안된 변경 사항
2002.4.2	감사 담당자는 조직의 독립성과 관련된 가능한 문제를 공개하고 이사회 또는 거버넌스 책임자들과 함께 이 문제를 논의해야 합니다. 감사 헌장에서 해결책을 찾고, 확인할 수 있어야 합니다

표준 1002 및 지침 2002를 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM01 거버넌스 프레임워크 설정 및 유지보수 보장	기업 거버넌스 접근방식에 통합되고 조정되어, 일관된 접근방식을 제공합니다. I&T 관련 결정은 기업의 전략 및 목적에 따라 이루어지고 원하는 가치가 실현됩니다. 이를 위해, I&T 관련 프로세스가 효과적이고 투명하게 감독되고, 법적, 계약적, 규제적 요구사항을 준수하는지, 그리고 이사회 구성원에 대한 거버넌스 요구사항이 충족되는지 확인합니다.
APO01 I&T 관리 프레임워크 관리	관리 프로세스, 조직 구조, 역할 및 책임, 신뢰할 수 있고 반복 가능한 활동, 정보 항목, 정책 및 절차, 기술 및 역량, 문화 및 행동, 서비스, 인프라 및 애플리케이션 등과 같은 거버넌스 구성요소를 포함하여, 기업 거버넌스 요건을 충족하기 위해 일관된 관리 접근방식을 구현합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

일반 표준 1003: 감사자 객관성

내용	**1003.1** IT 감사 및 보증 실무자는 감사 및 보증 업무와 관련된 모든 문제에서 객관적이어야 합니다.

일반 지침 2003: 감사자 객관성

이러한 지침은 IT 감사 및 보증 실무자들이 다음 작업을 수행할 수 있는 프레임워크를 제공합니다.

- 객관성이 훼손될 수 있는지 또는 훼손된 것으로 나타날 수 있는지 여부를 설정합니다.
- 객관성이 훼손되거나 훼손된 것으로 나타날 수 있을 때 감사 프로세스에 대한 잠재적인 다른 접근방식을 고려하십시오.
- 비감사 역할, 기능 및 서비스를 수행하는 IT 감사 및 보증 실무자들의 객관성 훼손이 미치는 영향을 줄이거나 없앱니다.
- 필요한 객관성이 훼손될 수 있는지 또는 훼손된 것으로 나타날 수 있을 때 공개 요건을 확인합니다.
- 보증 문제를 해결하고 결론을 내릴 때 공정하고 편파적이지 않은 태도로 IT 감사 또는 보증 업무여야 합니다.
- 모든 업무 단계에서 객관성에 대한 훼손 가능성을 염두에 두십시오.
- 객관성 훼손에 대한 세부정보를 해당 관계자에게 공개합니다.

2003.1 소개 지침은 다음과 같은 주요 IT 감사및보증 업무 주제 항목에 대한 정보를 제공하도록 구조화되었습니다.

2003.2 개념 프레임워크

2003.3 위협 및 보호장치

2003.4 위협 관리

2003.5 비감사 서비스 또는 역할

2003.6 독립성을 훼손시키지 않는 비감사 서비스 또는 역할

2003.7 독립성을 훼손시키는 비감사 서비스 또는 역할

2003.8 감사 헌장 및 비감사/자문 서비스 역할

2003.9 보고

2003.2 개념 프레임워크

2003.2.1	객관성 또는 독립성에 대한 위협을 평가할 때 다른 상황이나 상황의 조합이 관련될 수 있습니다. 객관성 또는 독립성에 위협을 야기하는 모든 상황을 정의하고 적절한 조치를 지정하는 것은 불가능합니다. 따라서, 이 지침은 전문가들이 객관성 또는 독립성에 대한 잠재적인 위협을 식별하고, 평가하고, 해결해야 하는 개념 프레임워크를 설정합니다. 개념 프레임워크 접근방식은 독립성 표준을 준수하는 데 도움을 주고, 독립성에 위협을 야기하는 상황에서의 많은 편차를 수용합니다.
2003.2.2	개념 프레임워크 접근방식은 실무자가 다음 작업을 수행할 경우 적용해야 합니다. • 객관성 또는 독립성에 대한 위협 식별 • 식별된 위협의 중요성 평가 • 필요한 경우 보호조치를 적용하여 위협을 없애거나 용인 가능한 수준으로 감소
2003.2.3	실무자들은 적절한 보호장치가 제공되지 않거나 객관성 위협을 없애거나 용인할 수 있는 수준으로 위협을 줄이는 데 적용할 수 없다고 판단할 경우, 위협을 야기하는 상황이나 관계를 제거하거나, 감사 또는 보증 업무를 거부하거나 종결해야 합니다. 실무자들이 업무를 거부하거나 종결할 수 없는 경우, 객관성이나 독립성에 대한 훼손을 거버넌스 책임자들에게 적절하게 공개하고 업무 결과 보고서에 포함해야 합니다.
2003.2.4	실무자들은 비감사 서비스 또는 역할을 수행할 때 ITAF 안내를 적용하여 객관성에 대한 잠재적 위협을 식별하고, 위협의 중요성을 평가하고, 적절한 보호장치를 구현할 것을 고려해야 합니다.
2003.2.5	감사자는 현재 또는 미래 감사 또는 보증 업무가 계획되어 있을 수 있고 동일한 감사자가 수행할 가능성이 높은 영역에서는 비감사 서비스 또는 역할을 수행해선 안됩니다. 기업에 다른 자원(즉, 대체 내부 또는 외부 자원을 참여시킴)이 없으면 비감사 서비스에 감사자의 관여는 최고감사임원(CAE)(또는 부사장/감사 이사) 및 공식적으로 거버넌스 및 감사 담당자 감독을 책임지는 이들(예: 이사회 및/또는 감사 위원회)에 의해 승인되어야 합니다.

2003.3 위협 및 보호장치

2003.3.1	광범위한 관계와 상황에서 객관성에 위협이 야기될 수 있습니다. 관계 또는 상황에서 위협을 야기할 때, 이러한 위협은 전문가의 객관성을 훼손하거나 훼손하는 것으로 인식될 수 있습니다. 상황이나 관계가 객관성에 한 가지 이상의 위협을 야기할 수 있습니다. 위협은 다음 범주 중 하나 이상에 속합니다. • **사리추구**—재정적 또는 기타 이익이 전문가의 판단이나 행동에 부적절하게 영향을 주는 위협 • **자체검토**—실무자가 자체적으로 또는 현재 업무에서 판단을 형성할 때 실무자들이 의지할 감사 담당자 내 다른 사람이 이전의 판단이나 수행된 서비스의 결과를 적절하게 평가하지 않을 위협 • **옹호**—실무자들이 피감인의 위치를 전문가의 객관성이 훼손되는 지점으로 진급시킨다는 위협 • **친근성**—피감인과의 오래되거나 가까운 관계로 인해, 실무자들이 피감인의 이익에 너무 동조하거나, 피감인의 작업, 관점 또는 주장을 너무 많이 받아들이게 될 위협 • **협박**—실무자들에게 부당한 영향력을 행사하려는 시도를 포함하여, 실제 또는 인식된 압력 때문에 실무자들이 무결성과 객관성을 가지고 행동하지 못하게 될 위협 • **편향**—정치적, 사상적, 사회적, 철학적 또는 기타 신념이 실무자들에게 영향을 주는 객관적이지 않은 입장을 취하도록 하는 위협 • **경영 참여**—실무자가 경영 역할을 맡음으로써 또는 감사 또는 보증 업무를 맡은 법인체 대신 경영 기능을 수행함으로써 발생하는 객관성 훼손의 위협

2003.3.2	객관성에 대한 위협을 줄이거나 최소화하기 위한 보호장치를 설계하고 구현할 수 있습니다. 식별된 위협에 대응하여 실무자들이 고려할 수 있는 보호장치의 예는 다음과 같습니다. • 기업 및 감사 기능 내에서 업무 배정에 있어서 객관적 선택을 보장하는 내부 절차(예: 감사자는 실무자가 이전에 직접 경영 책임을 가졌던 영역을 감사하지 않음) • 실무자를 보완하는 데 감사 기능 외부의 관리진 및 직원을 배정함(예: 다른 기능, 부서 또는 외부 조직의 직원 파견) • IT 감사 배정 정기 순환으로, 피감 영역의 사람들과 실무자의 친밀성을 줄임 • 실무자가 편향이나 이해충돌(즉, 경쟁 전문가 또는 개인적 이해)로부터 자유로울 수 있는 가능성을 높이기 위한 적절한 고용 관행(예: 배경 심사 및 조사) • 개인의 이해 또는 관계가 객관성에 위협을 가할 경우 업무에서 그 사람을 배제함 • 적절한 문서화 및 보고 요건으로, 전문가 독립성의 평가가 작업 서류로 문서화되고 산출물로 일관되게 보고되도록 함 • 이전에 참조된 감사 기능이나 기타 출처의 독립적인 자원을 할당하여 동료 검토를 수행하거나 계획, 현장 연구 및 보고 중 독립적인 관찰자 역할을 수행함 • 현장에서 인정된 권한이나 독립적인 전문가와 같이, 공인된 타사의 실무자에 의한 보고서, 통신 또는 정보의 외부 검토 산출

2003.4 위협 관리

2003.4.1	감사 담당자 및 실무자는 객관성에 대해 식별된 위협이 제거되었거나 수용 가능한 수준으로 줄었는지를 확인해야 합니다. 객관성 상실은 전문가 판단을 훼손하는 영향을 받지 않고 감사 또는 보증 업무를 수행하는 전문가의 능력에 영향을 줄 수 있거나, 객관성 상실로 인해 타당하고 정통한 제삼자가 IT 감사 및 보증 팀 구성원의 무결성, 객관성 또는 전문가적 의구심이 훼손되었다고 결론을 내리는 상황에 실무자 또는 감사 담당자가 놓일 수 있으므로, 객관성에 대한 위협을 관리해야 합니다.

2003.5 비감사 서비스 또는 역할

2003.5.1	많은 기업에서 경영진, IT 실무자 및 내부 감사 담당자는 실무자가 다음과 같은 비감사 서비스 또는 역할에 관여할 수 있을 것으로 기대합니다. • 기술, 애플리케이션 및 자원과 같은 영역과 관련된 IT 전략에서 자문 • 기술 평가, 선택 및 구현 • 타사 IT 애플리케이션 및 솔루션 평가, 선정, 커스터마이징 및 구현 • 맞춤형IT 애플리케이션 및 솔루션 설계, 개발 및 구현 • 다양한 IT 기능과 관련된 모범 사례, 정책 및 절차 수립 • IT 보안 및 IT 제어 설계, 개발, 테스트 및 구현 • IT 프로젝트에서 자문

2003.5.2	일반적으로 비감사 서비스 또는 역할 제공은 IT 기획 및 IT 프로젝트 팀에 전일제 또는 시간제 방식으로 참여하여 조언 또는 자문을 제공하는 것을 포함합니다. IT 감사 및 보증 실무자들은 다음과 같은 활동을 통해 비감사 기능을 이행할 수 있습니다. • IT 프로젝트 팀에 IT 감사 및 보증 실무자 전일제 임시 배정 또는 파견 • 프로젝트 관리(project steering) 그룹, 프로젝트 작업 그룹, 평가팀, 협상 및 계약팀, 구현팀, 품질 보증팀 또는 문제 해결팀과 같은 IT 프로젝트 구성원으로 IT 감사 및 보증 실무자 시간제 배정 • 필요에 따라, 그때그때 IT 프로젝트 또는 IT 제어 자문가 또는 검토자 역할 수행
2003.5.3	비감사 서비스 또는 역할 제공이 전문가의 객관성이나 독립성에 위협을 가하거나 비감사 서비스 또는 역할이 수행된 영역이 현재 감사 또는 보증 업무의 대상이거나 미래에 업무 대상이 되는 경우 이러한 위협이 나타나도록 할 수 있습니다. 이 상황에서는 실무자들의 독립성과 객관성이 모두 비감사 서비스 또는 역할 수행으로 훼손되었다는 인식일 수 있습니다.
2003.5.4	비감사 서비스 또는 역할을 제공하는 실무자들은 개념적 프레임워크를 사용하여 비감사 서비스 또는 역할이 현재 또는 미래 감사 또는 보증 업무의 객관성이나 독립성을 훼손하는지 여부를 평가해야 합니다. 이것은 비감사 서비스 또는 역할이 해당 업무의 주제 또는 이해관계자에게 유의미하거나중요한 영역에서 수행되는 업무에 적용됩니다. 필요한 경우, 실무자들은 IT 감사 및 보증 동료 및 관리진 및/또는 거버넌스 책임자에게서 지도를 받고 보호장치를 구현하여 객관성에 대한 실제 또는 인식된 위협을 적절하게 완화할 수 있는지 여부를 판별해야 합니다.
2003.5.5	비감사 서비스 또는 역할을 시행하기 전에, 실무자들은 IT 감사 관리진 및/또는 거버넌스 책임자와 다음에 관하여 적절하게 이해하고 문서화해야 합니다. • 비감사 서비스 또는 역할의 목적 • 수행될 비감사 서비스 또는 역할의 성격 • 비감사 서비스 또는 역할과 관련된 책임에 대한 피감인의 수용 • 비감사 서비스 또는 역할과 관련된 전문가 책임 • 비감사 서비스 또는 역할의 제한사항 • 미래 감사 서비스 실무자가 제공할 수 있는 범위에 대한 제한사항
2003.5.6	수행된 비감사 서비스 또는 역할로 인해 사고방식이나 겉모습에서 객관성 또는 독립성의 훼손 가능성이 있는 IT 감사 또는 보증 업무의 경우, IT 감사 및 보증 관리진은 다음과 같은 보호장치를 구현해야 합니다. • 면밀히 감사 시행 모니터링 • 수행된 비감사 서비스 또는 역할에서 발생되는 객관성 또는 독립성 훼손에 대한 중요한 징후를 평가하고 필요한 보호장치 개시 • 잠재적 객관성 또는 독립성 훼손과 구현된 보호장치에 대해 거버넌스 책임자에게 알림

2003.6 독립성을 훼손시키지 않는 비감사 서비스 또는 역할

2003.6.1	일상적인 관리이거나 일반적으로 중요하지 않은 문제와 관련된 활동은 경영 책임이 아닌 것으로 간주되므로, 객관성을 훼손하지 않습니다.
2003.6.2	적절한 보호장치가 구현되면 독립성 또는 객관성을 훼손하지 않는 비감사 서비스 또는 역할은 IT 위험 및 통제에서 일상적인 조언을 제공하는 일을 포함합니다.

2006.6.3	감사 또는 보증 업무의 대상인 (또는 될 수 있는) 영역에서 비감사 서비스 또는 역할을 제공할 때 경영 책임을 부담하는 위험을 막기 위해, 실무자들은 경영진이 비감사 서비스 또는 역할과 관련하여 다음 기능을 수행한 것 또는 수행할 것에 대해 만족하는 경우에만 비감사 서비스 또는 역할을 제공해야 합니다. ● 모든 경영 책임 부담 ● 가급적 고위 경영진 내에서 적합한 기술, 지식 또는 경험을 보유한 사람을 지명하여 서비스 감독 ● 수행된 서비스의 적절성 및 결과 평가 ● 서비스 결과에 대한 책임 감수 실무자들은 수행된 비감사 서비스 또는 역할을 효과적으로 감독하는 관리진의 능력을 고려함을 문서화해야 합니다.

2003.7 독립성을 훼손시키는 비감사 서비스 또는 역할

2003.7.1	실무자들이 경영 책임을 맡거나 경영 활동을 수행할 경우, 독립성에 대한 위협이 너무 커져서 어떤 보호장치로도 이러한 위협을 용인할 수 있는 수준으로 줄일 수 없게 될 수 있습니다. 활동이 경영 책임인지 여부는 상황에 따라 달라지며 전문가의 판단력을 발휘해야 합니다. 일반적으로 경영 책임으로 간주되는 활동의 예는 다음과 같습니다. ● 정책 및 전략적 방향 설정 ● 기업의 직원 행동을 지시하고 책임지기 ● 트랜잭션 권한 부여 ● 이행할 감사 담당자, 내부 감사 담당자, 조직, 회사 또는 기타 제삼자의 권고사항 결정 ● 내부 통제 설계, 이행 또는 유지관리 책임지기 ● IT 프로젝트 또는 계획 관리에 대한 책임 감수
2003.7.2	경영 책임을 맡는 것 외에도, 다음 비감사 서비스 또는 역할이 독립성 및 객관성을 훼손할 수 있습니다. ● 감사 또는 보증 업무의 주제에 중요하거나 중대한 정보 시스템을 설계, 개발, 테스트, 설치, 구성 또는 운영하는 작업의 감독 또는 수행에서 실무자의 중요한 관여 ● 감사 또는 보증 업무의 주제에 중요하거나 중대한 정보 시스템에 대한 통제 설계 ● 실무자들이 독립적으로 또는 공동으로 관리진 결정을 내리거나 정책 및 표준을 승인하는 책임을 지는 거버넌스 역할 이행 ● 경영 결정의 기본 기준을 정하는 조언 제공 또는 경영 기능 수행
2003.7.3	어떤 보호장치로도 수용할 수 있는 수준으로까지 줄일 수 없을 정도로 너무 큰 위협을 야기시켜, 객관성을 훼손할 것으로 간주되는 비감사 서비스는 다음과 같습니다. ● 경영 책임을 지거나 경영 활동 수행 ● 감사 또는 보증 업무의 주제에 중요하거나 중대한 정보 시스템을 설계, 개발, 테스트, 설치, 구성 또는 운영하는 작업의 감독 또는 수행에서 실무자의 중요한 관여 ● 현재 또는 계획된 미래 감사 업무의 주제에 중요하거나 중대한 정보 시스템에 대한 통제 설계 ● 실무자들이 독립적으로 또는 공동으로 관리진 결정을 내리거나 정책 및 표준을 승인하는 책임을 지는 거버넌스 역할 이행 ● 경영 결정의 기본 기준을 정하는 조언 제공

2003.8 감사 헌장 및 비감사 서비스/자문 역할

2003.8.1	IT 감사 헌장은 실무자들이 감사할 수 있는 기술과 관련하여 객관성이나 독립성 어느 것도 훼손되지 않도록 하기 위해 실무자들이 비감사 서비스 또는 역할을 수행할 수 있는지 여부와 이러한 서비스 또는 역할의 광의적 성격, 시기 및 범위를 설정해야 합니다. 이것은 사례별로 각 비감사 서비스 또는 역할에 대한 특정 권한을 얻어야 하는 필요성을 제거하거나 최소화할 수 있습니다.
2003.8.2	실무자는 특정 비감사 서비스 또는 역할의 운영 지침(TOR)이 감사 헌장을 준수한다는 합리적 확신을 제공해야 합니다. 모든 차이점은 TOR에 명시적으로 기술되어야 하며 IT 감사 및 보증 관리진 및/또는 거버넌스 책임자에 의해 승인되어야 합니다.
2003.8.3	감사 헌장이 비감사 서비스 또는 역할을 지정하지 않거나 감사 헌장이 없을 경우, 실무자들은 비감사 서비스 또는 역할에서 관여의 성격을 IT 감사 및 보증 관리진 및 거버넌스 책임자에게 보고해야 합니다. 비감사 서비스 또는 역할에서 실무자의 관여 시기 및 범위는 서비스 및 역할이 수행될 직능의 관리진이 서명하고 거버넌스 책임자가 승인한 개별 TOR에 따라야 합니다.

2003.9 보고

2003.9.1	IT 감사 또는 보증 업무를 수행하는 실무자들의 객관성이나 독립성이 훼손되거나 훼손될 수 있거나 훼손될 것으로 나타날 수 있는 경우, 그리고 거버넌스 책임자가 업무를 계속하도록 결정을 내린 경우, IT 감사 및 보증 업무 보고서는 보고서의 사용자가 잠재적 훼손의 성격을 이해할 수 있는 충분한 정보를 포함해야 합니다. 실무자들이 IT 감사 및 보증 업무 보고서에서 공개할 것을 고려해야 하는 정보는 다음과 같습니다. ● 객관성 또는 독립성의 훼손을 입었거나 입은 것으로 보일 수 있는 IT 감사 및 보증 업무에 관여한 실무자들의 이름과 근속 ● 객관성 또는 독립성에 대한 잠재적 훼손의 분석 및 설명 ● 참여 작업 및 보고 프로세스 과정에서 독립성과 객관성에 대한 다양한 위협을 제거하거나 완화하기 위해 구현된 보호장치 ● 거버넌스 책임자에게 객관성 또는 독립성의 잠재적 훼손을 공개하고 이러한 책임자가 보증 업무 및/또는 비감사 서비스 또는 역할을 수행하거나 계속하도록 승인한 사실의 문서화

표준 1003 및 지침 2003을 위한 COBIT® 2019 연결

COBIT 2019 관리 목표	목적
MEA02 내부 통제 시스템 관리	내부 통제 시스템의 적절성에 대한 주요 이해관계자들의 투명성을 확보하여 운영에 대한 신뢰, 기업 목표 달성에 대한 확신, 그리고 잔여 위험에 대한 적절한 이해를 제공합니다.
MEA03 외부 요건 준수 관리	기업에 적용되는 모든 외부 요건을 준수하도록 합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

일반 표준 1004: 합리적 기대

내용	**1004.1** IT 감사 및 보증 실무자는 해당 IT 감사 및 보증 표준과 필요 시 기타 산업 표준 또는 해당 법과 규정에 의거하여 업무를 완료하여 전문가 의견이나 결론을 도출할 수 있다는 합리적인 기대를 가져야 합니다.
	1004.2 IT 감사 및 보증 실무자는 업무의 범위를 통해 해당 주제에 대한 결론을 낼 수 있고, 범위 제한이 지정된다는 합리적인 기대를 가져야 합니다.
	1004.3 IT 감사 및 보증 실무자는 경영진이 업무를 수행하는 데 필요한 적절하고 관련성 있고 시기적절한 정보를 제공하는 것과 관련하여 의무와 책임을 이해한다는 합리적인 기대를 가져야 합니다.

일반 지침 2004: 합리적 기대

2004.1 소개 이 지침의 목적은 감사 업무의 실행에서 합리적인 기대 원칙을 구현하는 과정에서 IT 감사 및 보증 실무자를 지원하기 위한 것입니다. 뿐만 아니라, 이 지침은 범위 제한을 지정하는 데 IT 감사 및 보증 실무자를 지원하고, 업무 조건의 변경을 승인하는 과정을 안내합니다.

2004.2 표준 및 규정

2004.3 범위

2004.4 범위 제한

2004.5 정보

2004.6 업무 조건의 변경 수락

2004.7 기타 고려사항

2004.2 표준 및 규정

2004.2.1	실무자들은 감사 업무 전에 감사 헌장 및 규정에 나열된 모든 해당 표준을 취합해서 평가하고, 전체 업무 기간 동안 이러한 표준을 재확인하여 이러한 표준 및 규정에 따라 감사 업무를 완료할 수 있다는 합리적 기대를 가지는지 여부를 판별하고, 감사 업무가 전문가 의견이나 결론으로 귀결되도록 해야 합니다.
2004.2.2	실무자들이 하나 이상의 해당 표준 및 규정에 따라 감사 업무를 완료할 수 없고, 그렇기 때문에 전문가 의견이나 결론을 표현할 수 없다고 판단하는 경우, • 실무자들은 IT 감사 및 보증 관리진 및 거버넌스 책임자들에게 확인된 표준 및 규정 준수 문제를 알려야 합니다. • 실무자들은 업무 조건의 변경을 제안하거나 또는 제안된 업무를 거부해야 합니다.

2004.3 범위

2004.3.1	감사 업무를 수행하기 전에 실무자들은 감사의 범위가 명확히 문서화되는지 파악하고, 주제 사안에 대해 전문가 의견이나 결론이 도출된다는 것을 허용해야 합니다.
2004.3.2	감사 업무의 범위는 업무 범위에 어떤 영역(예: 프로세스, 활동, 시스템)이 있는지에 대해 해석의 여지 없이, 명확히 문서화되어야 합니다. 범위가 너무 모호하게 기술되면 범위의 모든 영역이 평가되었다는 확실성이 결여되기 때문에 실무자들은 전문가 의견이나 결론을 구성할 수 없습니다.
2004.3.3	실무자들이 감사 업무의 범위가 전문가 의견이나 결론을 표현할 수 없다고 판단할 경우: • 실무자들은 IT 감사 및 보증 관리진 및 감사 기능의 거버넌스 책임자들에게 확인된 범위 문제를 알려야 합니다. • 실무자들은 업무 조건의 변경을 제안하거나 또는 제안된 업무를 거부해야 합니다.

2004.4 범위 제한

2004.4.1	특정 범위 제한은 감사 업무 전 또는 과정에서 발생할 수 있습니다. 이러한 범위 제한은 다음과 같은 여러 요인의 영향을 받을 수 있습니다. • 감사 업무를 완료하는 데 필요한 적절하고, 관련되고, 시기 적절한 정보를 사용할 수 없습니다. • 주요 피감인을 확보할 수 없습니다. • 할당된 시간이 전체 감사 업무 범위를 완료하기에 충분하지 않습니다. • 경영진이 감사 업무의 범위를 선택한 영역으로 제한하려고 합니다. • 감사 업무의 범위가 주제 사안에 대한 결론을 내기에 너무 작거나 너무 큽니다. • 분산화 수준 때문에 주제 사안의 총체성에 대한 결론에 도달하기 어렵습니다. • 현재 범위로 감사 업무를 수행할 수 있는 적절한 기술을 가진 실무자 수가 충분하지 않습니다. • 감사 담당자의 보고 구조(예: 감사 담당자가 기업 내 적절한 수준에 보고하지 않으면 범위의 특정 요소를 평가하지 않도록 지시할 수 있음). • 타사 계약은 범위 제한이 받아들여 질 수 있습니다. • 클라이언트 문서 제공이 지연됩니다. • (이전 감사에서 식별되거나 피감인이 자체 식별한) 기존의 비적합성에 대한 수정이 여전히 처리 중입니다.
2004.4.2	실무자들은 범위 제한에도 감사 업무가 전문가 의견이나 결론을 도출할 것이라는 합리적 기대를 할 수 있는지 여부를 고려해야 합니다. 실무자들이 이 조건이 충족되지 않을 것이라고 판단하면, 업무를 수락해선 안됩니다.
2004.4.3	실무자들이 범위 제한에도 불구하고, 업무에서 전문가 의견이나 결론이 도출될 것이라는 합리적 기대를 여전히 가지고 있다고 결론 지으면, 실무자들은 감사 업무를 수락하거나 계속해야 합니다. 범위 제한은 IT 감사 및 보증 업무 보고서에 명확하게 기술되어야 합니다.
2004.4.4	범위가 주제 사안에 대해 표현되어야 할 감사자의 의견을 허용할 만큼 충분한지 고려해야 합니다. 범위 제한이 발생할 수 있는 경우는 업무 완료에 필요한 정보가 없거나, IT 감사 또는 보증 업무에 포함된 일정이 촉박하거나, 경영진이 선택된 부문으로 범위를 제한하려고 할 때입니다. 이러한 경우, 통제 검토, 필요한 표준 및 관행 준수, 계약서, 라이센스, 법률, 규정 준수 등 다른 유형의 활동이 고려될 수 있습니다.

2004.5 정보

2004.5.1	감사 헌장은 감사 업무 수행과 관련된 정보, 시스템, 인력 및 위치에 대한 접근 권한을 지정합니다.
2004.5.2	감사 업무를 수행하기 전에 실무자들은 감사 업무에 대한 적절하고 관련되고 시기적절한 정보에 대한 접근 권한에 부여된 제한사항을 식별하고 해결해야 합니다. 감사 실무자들은 감사 업무에 대한 접근 권한이 감사 헌장의 조항을 따르거나, 조항에서 벗어날 수 있는 경우, 실무자들이 주제 사안에 대한 전문가 의견이나 결론에 도달하는 것을 방해하지지 않을 것이라는 합리적 기대를 가져야 합니다.
2004.5.3	감사 실무자들이 정보에 대한 접근 권한으로 전문가 의견이나 결론을 표현할 수 없다고 결론 내릴 경우: ● 감사 실무자들은 IT 감사 및 보증 관리진 및 감사 기능 거버넌스 책임자에게 적절하고 관련성이 있으며, 그리고 시기적절한 정보의 접근 권한에 관하여 확인된 문제를 알립니다. ● 업무 조건의 변경을 제안하거나 또는 제안된 감사 업무를 수락해선 안 됩니다.
2004.5.4	감사 또는 보증 업무 수행은 경영진이 수행하는 활동의 평가를 포함할 수 있습니다. 감사 업무를 실행하기 전에 그 가능성을 평가해야 합니다. 감사 실무자들은 이러한 인사 또는 관련 정보에 접근을 시도할 필요가 있는지 여부를 평가해야 합니다. 감사 업무를 실행하기 전 필요할 수 있는 완화 조치는 다음과 같습니다(단, 이에 제한되지는 않음). ● 감사 담당자 및 전문가에게 적절한 권한을 할당하는 감사 헌장 규정 ● 거버넌스 책임자(예: 이사회 및 감사 위원회)로부터 명시적 서면 지원 ● 경영진 또는 고위 관리직에 접근이 필요한 경우 이사회 또는 고위 관리직의 참석

2004.6 업무 조건의 변경 수락

2004.6.1	실무자들은 전문가적 판단에서 감사 업무 조건을 변경할 정당성이 없다고 생각되면 이러한 변경을 수락해선 안됩니다.
2004.6.2	감사 업무 과정에서, 실무자들에게 보증 수준을 낮추는 조건의 변경을 수락할 것을 요청하면, 전문가적 판단을 토대로 그렇게 할 정당성이 있는지 여부를 판별해야 합니다.
2004.6.3	감사 업무의 조건이 변경되면 실무자와 IT 감사 및 보증 관리진 양측이 기록하고 공식적으로 승인해야 합니다. IT 감사 및 보증 업무 보고서는 이 조건의 변경을 명시적으로 언급해야 합니다.
2004.6.4	실무자들이 감사 업무 조건의 변화를 수락하지 않고 경영진이 원래 감사 업무를 계속할 것을 허가하지 않으면 감사 및 보증 관리진과 협의하여, ● 실무자들은 감사 업무에서 철회해야 합니다. ● 실무자들은 전문가의 판단에 따라, 거버넌스 책임자(예: 이사회 또는 규제자)에게 상황을 보고할 지 여부를 판별해야 합니다.

2004.7 기타 고려사항

2004.7.1	IT 감사 및 보증 감사 실무자는 다음을 수행해야 합니다. • 업무가 전문적 표준에 의거하여 성공적으로 완료될 수 있을 때만 IT 감사 또는 보증 업무를 수행해야 합니다. • 업무의 주제 사안이 해당 기준에 비추어 평가될 수 있을 때만 IT 감사 및 보증 업무를 수행해야 합니다. • IT 감사 또는 보증 업무의 범위를 검토함으로써 범위가 분명히 문서화되어 피감인들에게 명확히 전달될 수 있음을 확인해야 합니다. • 적절하고 관련성이 있으며 그리고 시기적절한 정보에 대한 접근을 포함하여(이에 제한되지 않음), 수행될 업무에 가해진 제한사항을 식별하고 해결해야 합니다. • 피감사 책임 경영진으로부터 서면 기술서를 얻을 수 없는 경우 준비해야 합니다. 예를 들어, 구두 기술서를 확보하여 업무 서류로 문서화할 수 있습니다.

표준 1004 및 지침 2004를 위한 COBIT® 2019 연결

COBIT 2019 관리 목표	목적
MEA03 외부 요건 준수 관리	기업에 적용되는 모든 외부 요건을 준수하도록 합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

일반 표준 1005: 정당한 주의의무

내용	**1005.1** ISACA의 직업윤리강령에 따라, 감사자들은 주의의무를 가지고 전문적인 방식으로 임무를 수행합니다. 이들은 높은 수준의 행동과 인격을 유지할 것이며, 그들 자신이나 직업의 신뢰를 훼손시킬 수 있는 행위에 관여하지 않도록 합니다. 감사자의 임무 수행 과정에서 얻은 정보의 개인정보 보호 및 기밀성을 유지해야 합니다. 뿐만 아니라, 이 정보는 개인의 이익에 사용하거나 법적 기관에서 요구하는 경우가 아니면 공개해선 안됩니다.

일반 지침 2005: 정당한 주의의무

2005.1 “정당한 주의의무” 용어는 ISACA 직업윤리강령을 준수하여 무결성을 가지고 신중하게 감사 업무를 계획, 수행 및 보고하는 데 적용되므로, 본 지침의 목적은 이 용어를 명확히 하는 것입니다. 정당한 주의의무는 무과실성이나 뛰어난 수행이 아니라, 합당한 신중함과 역량을 암시합니다.

2005.2 전문가적 의구심 및 역량

2005.3 적용

2005.4 업무 수명 주기

2005.5 통신

2005.6 정보 획득 및 관리

2005.7 기타 고려사항

2005.2 전문가적 의구심 및 역량

2005.2.1	정당한 주의의무는 업무 수행에서 전문가 판단력을 행사하는 데 적용됩니다. 정당한 주의의무는 실무자들이 전문가 판단이 필요한 문제를 전문가적 의구심을 가지고, 성실하게 무결성을 가지고 신중하게 접근해야 함을 암시합니다. 이들은 전체 업무 기간 동안 이러한 태도를 유지해야 합니다.
2005.2.2	실무자들은 감사 업무 수행과 관련된 모든 문제에서 생각과 외관 모두에서 역량, 객관성 및 독립성을 유지해야 합니다. 그들은 문제를 해결하고 결론에 도달하는 데 정직하고 공정하고 편파적이지 않아야 합니다.
2005.2.3	정당한 주의의무를 이행할 때 실무자들은 비효율성, 오용, 오류, 범위 제한, 기술 부족, 이해 충돌 또는 사기 행위의 존재 가능성을 고려해야 합니다. 또한 실무자들이 이러한 문제가 발생할 수 있는 특정 조건이나 활동에 주의를 기울이도록 해야 합니다.
2005.2.4	실무자들은 전문가 표준 개발을 계속 알리고 준수하여 IT 감사 및 보증 목적을 달성하기에 충분한 이해와 전문가 역량을 보여주어야 합니다.
2005.2.5	실무자들은 전문가 표준과 법정 및 규정 요건을 준수하면서 성실하게 감사 업무를 수행해야 합니다.

2005.3 적용

2005.3.1	정당한 주의의무는 감사 위험 평가, 감사 과제 수락, 감사 범위 설정, 감사 목적 정립, 감사 계획, 감사 시행, 감사에 자원 할당, 감사 테스트 선택, 테스트 결과 평가, 감사 문서화, 감사 결론 도달, 감사 결과 보고 및 제공, 사후 활동 시행을 포함하여(이에 제한되지 않음) 감사의 모든 측면으로 확장되어야 합니다. 이를 수행할 때, 실무자들은 다음 사항을 확인하거나 평가해야 합니다. • IT 감사 및 보증 표준을 충족하는 데 필요한 자원의 유형, 수준, 기술 및 역량 • 감사 주제에서 식별된 위험의 중요도 및 이러한 위험의 잠재적 영향 • 수집된 감사 증거의 충분성, 유효성 및 관련성 • 작업 실무자들이 의존하는 다른 이들의 역량, 무결성 및 결론
2005.3.2	또한 정당한 주의의무에서는 실무자들이 합리적 확신 개념을 가지고 모든 업무를 수행할 것을 요구합니다.
2005.3.3	실무자들은 높은 수준의 행위와 품격을 유지하면서 합법적이고 정직한 방식으로 관련 당사자의 이익을 위해 일하고, 해당 직업의 신뢰를 떨어뜨리는 행위에는 관여하지 말아야 합니다.

2005.4 업무 수명 주기

2005.4.1	실무자들은 정당한 주의의무에 따라 적절한 자원 가용성과 적시에 감사 업무 완료를 보장함으로써 완전하고 시기 적절하게 감사 업무를 계획해야 합니다. 프로젝트에 할당된 실무자들은 감사 업무를 수행하는데 필요한 기술, 지식 및 관련 역량을 총체적으로 보유해야 합니다.
2005.4.2	감사 실무자들은 정당한 주의의무를 적용하여, 즉 적절한 전문가 표준에 따라 품질과 완전한 감사 결론 또는 의견을 보장하여 감사 업무를 수행해야 합니다.
2005.4.3	감사 실무자들은 경영진의 시정조치가 감사에서 얻은 결과를 효과적으로 다루는지 확인하는데 정당한 주의의무를 이행해야 합니다.

2005.5 통신

2005.5.1	감사 업무 중 팀이 적절한 전문가 표준을 준수함을 보장하기 위해서는 프로젝트가 시작되기 전에 정의된 역할과 책임을 팀 구성원들에게 전달해야 합니다.
2005.5.2	감사 업무 중, 실무자들은 피감인 및 관련 이해관계자들과 적절하게 소통하여 협조하도록 해야 합니다.
2005.5.3	실무자들은 감사 업무의 피감인들에게 결과를 전달해야 합니다.
2005.5.4	실무자들은 이러한 문제를 해결하기 위해 전문가 표준 적용에 관한 문제를 문서화하고 해당 당사자들에게 전달해야 합니다.
2005.5.5	실무자들은 해당 당사자에게 수행된 작업 결과를 알릴 때 정당한 주의의무를 이행해야 합니다.

2005.6 정보 획득 및 관리

2005.6.1	감사 실무자들은 경영진이 감사 업무 수행에 필요한 적절하고 관련되고 시기 적절한 정보를 제공해야 하는 의무와 책임을 이해한다는 합리적 기대를 가지고 있어야 합니다.
2005.6.2	감사 실무자들은 사법 당국에 의해 공개가 요구되지 않는 한 임무 수행 과정에서 습득한 정보의 프라이버시와 기밀성을 유지하기 위한 타당한 조치를 취해야 합니다. 이러한 정보는 개인적인 목적으로 사용하거나 부적절한 대상에게 공개해선 안됩니다.
2005.6.3	조직의 정책 및 관련 법, 규칙 및 규정에 따라 정보를 얻고, 사용하고, 보유하고 적절하게 공개해야 합니다.

2005.7 기타 고려사항

2005.7.1	IT 감사 및 보증 감사 실무자는 다음을 수행해야 합니다. ● 무결성과 신중함을 바탕으로 활동을 수행해야 합니다. ● 업무 목적을 달성하기 위한 충분한 이해와 역량을 보여주어야 합니다. ● 전체 업무 기간 동안 전문가적 의구심을 유지해야 합니다. ● 전문성 표준에 대한 지식을 지속적으로 갖추고 준수함으로써 전문가로서의 역량을 유지해야 합니다. ● 팀원들에게 팀 역할과 책임을 알리고, 팀이 업무 수행 시 해당 표준을 준수하도록 해야 합니다. ● 업무 수행 중 표준 적용에 관한 모든 문제를 해결해야 합니다. ● 전체 업무 기간 중 관련 이해관계자들과 효과적인 소통을 유지해야 합니다. ● 업무 기간 중에 승인 받지 않은 당사자에게 우연히 알려지거나 공개됨으로써 획득 및 파생된 정보를 보호하기 위한 합리적 수단을 취해야 합니다. ● 합리적 확신의 개념을 가지고 모든 업무를 수행해야 합니다. 테스트 수준은 업무 유형에 따라 다릅니다. ● 관련 기술 및 데이터 분석 기법의 사용과 기술 및 기법을 사용하는 감사자의 역량을 고려합니다. ● 잠재적 이익과 관련된 업무 비용을 고려합니다.

표준 1005 및 지침 2005를 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM01 거버넌스 프레임워크 설정 및 유지보수 보장	기업 거버넌스 접근방식에 통합되고 조정되어, 일관된 접근방식을 제공합니다. I&T 관련 결정은 기업의 전략 및 목적에 따라 이루어지고 원하는 가치가 실현됩니다. 이를 위해, I&T 관련 프로세스가 효과적이고 투명하게 감독되고, 법적, 계약적, 규제적 요구사항을 준수하는지, 그리고 이사회 구성원에 대한 거버넌스 요구사항이 충족되는지 확인합니다.
APO07 인적 자원 관리	기업 목적을 달성할 수 있도록 인적 자원 역량을 최적화합니다.
MEA03 외부 요건 준수 관리	기업에 적용되는 모든 외부 요건을 준수하도록 합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

일반 표준 1006: 숙련성

내용	**1006.1** 감사 및 보증 업무 보조자와 총칭해서, IT 감사 및 보증 실무자는 필요한 작업을 수행할 수 있는 전문적 역량을 갖추어야 합니다.
	1006.2 IT감사 및 보증 실무자들은 IT 감사 및 보증 업무에서 자신들의 역할을 수행하기 위해 해당 주제에 대한 적절한 지식을 가지고 있어야 합니다.
	1006.3 IT 감사 및 보증 실무자는지속적으로 적절한 직무 교육과 훈련을 통하여 전문직 종사자로서의 전문성을 유지해야 합니다.

일반 지침 2006: 숙련성

2006.1 소개 본 지침은 IT 감사 및 보증 실무자들이 감사 업무를 수행함에 있어 전문가적 역량을 유지하며 요구되는 기술과 지식 습득에 도움이 되도록 합니다. 지침 내용 섹션은 다음과 같은 주요 IT 감사 및 보증 업무 주제에 대한 정보를 제공하도록 구성되었습니다.

2006.2 전문가 역량

2006.3 평가

2006.4 원하는 수준의 역량에 도달

2006.5 기타 고려사항

2006.2 전문가 역량

2006.2.1	전문가 역량은 적정한 수준의 교육과 경험을 통해 감사 업무를 적절하게 수행하기 위한 기술, 지식 및 전문 기술의 보유를 나타냅니다.
2006.2.2	IT 감사 및 보증 관리진은 감사 업무의 여러 역할에 대해, 적절한 벤치마크에 근거한, 요구 및 기대 수준 역량을 갖춘 전문가들과 소통하여야 하며, 해당 벤치마크가 주기적으로 검토되고 갱신되도록 해야 합니다. IT 감사 및 보증 관리진은 여러가지 업무/직위에 요구되는 전문가 역량을 문서화 하여야 합니다. 예를 들면, 업무/직위 명세 문서화 혹은 다양한 직위에 필요한 전문가 역량을 보여주는 도식표 작성 등 입니다.
2006.2.3	IT 감사 및 보증 관리진은 IT 감사 계획에 정의된 감사 업무 수행에 요구되는 핵심자원 가용성에 대한 적정한 확인을 하여야 합니다. 핵심자원 가용성은 감사업무 시행 개시 이전에 확인 및 확정 되어야 합니다.
2006.2.4	IT 감사 및 보증 관리진은 팀원들이 감사 업무를 수행할 수 있는 능력이 있음을 보장해야 합니다. 팀원들의 핵심 전문가 역량 파악은 가용 자원의 효율적 활용에 도움이 될 것입니다.
2006.2.5	실무자들은 필요수준의 전문가 역량을 보유하였음에 대한 타당한 증빙을 제공해야 합니다. 이들은 자신들이 이행을 동의한 모든 임무를 수행함에 있어 요구되는 전문적이고 숙련된 기술과 지식을 채득하여야 합니다.
2006.2.6	실무자들에게 요구되는 기술과 지식은 감사 업무에서의 직무와 역할에 따라 달라집니다. 관리 기술과 지식에 대한 요건은 책임 수준에 비례해야 합니다.
2006.2.7	기술 및 지식은 위험 및 통제 식별과 평가에서의 능숙도 뿐만 아니라, 감사 도구 및 기법의 적용과 사용에서의 능숙도 또한 포함합니다. 실무자들은 인터뷰, 대인관계 및 프리젠테이션 기술과 함께 분석 및 기술 지식을 보유해야 합니다.
2006.2.8	실무자들은 감사 업무에 있어 편향된 자료 또는 적절한 조건들의 영향도를 식별하고 판단할 수 있는 지식을 보유하고 있어야 합니다.
2006.2.9	실무자들은 가능한 사기지표를 인식하는 능력을 보유해야 합니다.
2006.2.10	정보기술 지식뿐만 아니라, 실무자들은 잠재적 문제나 결점을 간과하지 않도록 하기 위해 경제학, 금융, 회계, 위험, 세금 및 법 등의 비즈니스 기본사항을 대한 일반적인 지식을 가지고 있어야 합니다.
2006.2.11	감사 실무자들이 전문 역량을 향상시키기 위해 팀원들과 함께 경험, 채택된 모범 사례, 교훈 및 습득 지식을 공유하는 것이 적합합니다. 팀원들의 전문가 역량은 팀 구성 세션, 워크샵, 회의, 세미나, 강의 및 기타 상호작용 모드를 통해 향상됩니다.
2006.2.12	적절한 기술 가용성을 보장하려면, 특정 자원 하위 계약, IT 감사 및 보증 작업의 일부 아웃소싱 또는 필요한 기술을 사용할 수 있을 때까지 감사 업무를 지연시키는 등 적절한 기술을 획득하기 위한 다른 대안이 고려되어야 합니다.
2006.2.13	업무의 일부 또는 전부를 아웃소싱하여 외부의 전문 지식을 얻을 수 있습니다. 아웃소싱된 자원과 내부 실무자들 간의 협업은 지식과 기술이 개발되고 내부적으로 유지보수 되도록 합니다.
2006.2.14	감사업무 일부가 아웃소싱되거나 전문가 지원이 필요한 경우에는 아웃소싱 기관이나 외부 전문가가 요구되는 전문적 역량을 보유 하였다는 타당한 확증을 제공 받아야 합니다.
2006.2.15	지속적으로 전문가 지원을 받는경우 해당 전문가의 전문역량은 주기적으로 업계 표준 또는 벤치마크를 기준으로 조사, 측정 및 검토 되어져야 합니다.

2006.3 평가

2006.3.1	실무자들은 지속적으로 기술과 지식을 모니터링하여 적절한 수준의 전문가 역량을 유지해야 합니다. IT 감사 및 보증 관리진은 주기적으로 전문가 역량을 평가해야 합니다.
2006.3.2	실무자들의 수행 평가는 공정하고, 투명하고, 쉽게 이해되고, 모호하지 않고 편향되지 않고, 고용 환경을 고려할 때 일반적으로 용인되는 실무수행으로 간주되는 방식으로 수행되어야 합니다.
2006.3.3	평가 기준 및 절차는 분명하게 정의되어야 하지만, 지리적 위치, 정치적 분위기, 배정 성격, 문화 및 기타 유사한 상황과 같은 상황에 따라 달라질 수 있습니다.
2006.3.4	실무자 팀의 경우, 평가는 팀 또는 협업 관계의 개인들 간에 내부적으로 수행되어야 합니다.
2006.3.5	독립적인 단일(단독) 실무자의 경우, 가능한 범위까지 동료 평가를 수행해야 합니다. 동료 평가가 가능하지 않다면, 자체 평가를 실시하고 문서화해야 합니다.
2006.3.6	실무자 성취도 평가는 적합한 수준의 관리진에 의해 수행되어야 합니다.
2006.3.7	평가 중 지적된 간극을 적절하게 해결해야 합니다.

2006.4 원하는 수준의 역량에 도달

2006.4.1	실제 수준의 전문가 역량과 기대한 수준의 전문가 역량 간의 차이에 기반한 간극을 기록하고 분석해야 합니다. 중요 결함이 자원에 있을 경우, 그 자원은 감사 업무를 수행하는 데 사용되어선 안 됩니다.
2006.4.2	간극의 원인을 알아내고 가능한 한 빨리, 교육 및 계속적 전문 교육(CPE) 등과 같은 적절한 정정 조치를 취하는 것이 중요합니다.
2006.4.3	감사 업무에 필요한 교육 활동은 합당한 시간 내, 그리고 감사 활동 시행 전에 완료되어야 합니다.
2006.4.4	교육의 효과성은 교육 완료 시 측정되어야 합니다.
2006.4.5	IT 감사 및 보증 관리진이 만든 대로, 숙련도 매트릭스 등의 필요한 숙련도의 문서화는 간극과 교육 필요성을 식별하는데 유용합니다. 매트릭스는 사용 가능한 인력 및 그 인력의 기술 및 지식과 상호 참조할 수 있습니다.
2006.4.6	제공된 교육 레코드는 교육에 대한 피드백 및 교육의 효과성과 함께, 유지보수되고 분석되고 추후 사용시 참조되어야 합니다.
2006.4.7	CPE는 ISACA가 전문가 역량을 유지보수하고 기술과 지식을 업데이트하기 위해 채택한 방법론입니다.
2006.4.8	CPE 프로그램은 IT 감사, 위험, 보안, 개인정보 보호 및 거버넌스의 전문가 및 기술적 요구사항과 관련된 기술 및 지식을 향상시키는데 도움을 주어야 합니다. 전문가 기구는 일반적으로 CPE 인정을 받을 수 있는 프로그램을 지정합니다. 실무자들은 각 전문가 기구에서 규정한 규범을 준수해야 합니다.
2006.4.9	전문가 기구는 일반적으로 CPE 신뢰와 기관 구성원이 주기적으로 얻어야 하는 최소 신용을 얻기 위한 방법론을 규정합니다. 실무자들은 각 전문가 기구에서 규정한 규범을 준수해야 합니다. 실무자들이 최소 신용을 얻기 위한 목적으로 둘 이상의 전문가 기구와 연관되어 있을 때, 각 전문가 기구가 정한 규칙/지침과 일치할 경우 실무자들은 전문가의 판단을 사용하여 적합한 프로그램에서 공통된 방식으로 CPE 점수를 얻을 수 있습니다.
2006.4.10	ISACA는 CISA 자격의 구성원 및 소유자에게 해당되는 CPE에 대한 포괄적인 정책을 가집니다. CISA 지명을 받은 실무자들은 ISACA의 CPE 정책을 준수해야 합니다. 정책 세부사항은 *www.isaca.org/credentialing/cisa/maintain-cisa-certification*에서 찾을 수 있습니다.
2006.4.11	ISACA를 포함하여, 각 전문가 기구에서 규정한 대로, 실무자들은 CPE 프로그램의 적절한 레코드를 유지관리하고, 특정 기간 동안 레코드를 보유하고, 필요한 경우 감사에 사용할 수 있게 해야 합니다.

2006.5 기타 고려사항

2006.5.1	IT 감사 및 보증 감사 실무자는 다음을 고려해야 합니다. • 작업을 수행하기 전에 충분한 전문가 역량을 보유하고 있음을 증명해야 합니다(계획된 업무와 관련된 기술, 지식 및 경험). • 적절한 기술 가용성을 보장하려면, 특정 자원 하위 계약, IT 감사 및 보증 작업의 일부 아웃소싱 또는 필요한 기술을 사용할 수 있을 때까지 감사 업무를 지연시키는 등 적절한 기술을 획득하기 위한 다른 대안을 고려해야 합니다. • IT 감사 및 보증 업무에 참여한 팀원들은 CISA 또는 기타 관련 전문 자격을 가지고 있고 충분한 공식 교육, 훈련 및 작업 경험을 가지고 있는지 확인해야 합니다. • IT 감사 또는 보증 업무를 이끌 때는 모든 팀원에게 기대하는 작업 수행을 위한 적합한 수준의 전문가 능력이 있다는 합리적 확신을 제공해야 합니다. • 다른 팀원 및 관련 전문가들과 함께 IT 감사 또는 보증 업무를 효과적이고 효율적으로 진행할 수 있도록 주요 분야에 대해 충분한 지식을 보유해야 합니다. • 지속적인 전문가 교육이나 CISA 또는 기타 관련 전문가 인증 개발 요건을 충족해야 합니다. • IT 감사 또는 보증 역할의 요건에 상응하는 수준의 전문가 서비스를 제공할 수 있도록 교육 과정, 세미나, 컨퍼런스, 웹캐스트, 직무 연수를 통해 전문적 지식을 지속적으로 쌓아야 합니다. • 필요한 역량을 필요한 시간에 사용할 수 있게 된다면, 외부 자원을 사용하여 업무를 수용할 것을 고려하십시오.

표준 1006 및 지침 2006을 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM04 자원 최적화 보장	기업의 자원 요구가 최적의 방식으로 충족되고, I&T 비용이 최적화되고, 이익 실현 가능성이 높아지고 미래 변화에 대비되도록 해야 합니다.
APO07 인적 자원 관리	기업 목적을 달성할 수 있도록 인적 자원 역량을 최적화합니다.

일반 표준 1007: 의견 표명

내용	**1007.1** IT 감사 및 보증 실무자는 감사 주제가 평가될 때 기준이 되는 의견 표명을 검토하여, 해당 의견 표명이 감사 대상 자질이 있는지 및 의견 표명이 충분하고, 유효하며, 적절한지를 파악해야 합니다.

일반 지침 2007: 의견 표명

2007.1 소개 이 지침의 목적은 다양한 의견 표명을 상세히 기술하고, 감사 주제가 평가될 기준이 의견 표명을 뒷받침하도록 IT 감사 및 보증 실무자를 안내하고, 결론을 도출하고 의견 표명에 대한 보고서를 작성하기 위한 지침을 제공하는 것입니다. 지침 섹션은 다음과 같은 주요 IT 감사 및 보증 주제에 대한 정보를 제공하도록 구조화되었습니다.

2007.2 의견 표명

2007.3 감사 주제 기준

2007.4 제3자가 제시한 의견 표명

2007.5 결론 및 보고서

2007.6 기타 고려사항

2007.2 의견 표명

2007.2.1	의견 표명은 감사 주제가 선택한 기준에 기반하거나 따르는지 여부에 대한 선언 또는 일련의 선언입니다. 감사 실무자들은 전체 감사 업무 실행 과정에서 이러한 의견 표명을 고려하고, 그들의 업적에 대한 보증을 얻고, 감사 보고서에 이를 언급해야 합니다.
2007.2.2	고려할 수 있는 공통된 의견 표명은 다음과 같습니다. • **기밀성**—개인정보 보호 및 소유권 정보 보호에 대한 접근 수단을 포함하여, 정보 접근 및 공개에 대한 승인된 제약 사항의 준수. • **완전성**—기록되어야 하는 모든 활동, 정보 및 기타 데이터가 기록됩니다. 예를 들어, 운영으로 이관된 모든 IT 시스템 변경 사항은 변경 관리 추적 애플리케이션에서 기록됩니다. • **정확성**—기록된 활동과 관련된 금액, 날짜 및 기타 데이터가 적절하게 기록되었습니다. 예를 들어, 운영으로 이관된 IT 시스템 변경 사항과 관련된 데이터는 변경 관리 추적 애플리케이션의 변경 레코드에 정확하게 표시됩니다. • **무결성**—수신된 정보, 증거 및 기타 데이터는 신뢰할 수 있고 믿을 수 있는 출처에서 제공되며 전체 수명 주기 동안 보호됩니다. 예를 들어, 백업이 완료된 후 해시를 백업 직전 해시와 비교하는 것은 부당 변경 여부를 확인하기 위한 것입니다. • **가용성**—감사 업무에 필요한 정보, 증거 및 기타 데이터가 존재하고 접근할 수 있습니다. 예를 들어, 요청된 변경 레코드가 존재하고 변경 관리 추적 애플리케이션에서 쉽게 접근할 수 있습니다. • **법규 준수**—정보, 증거 및 기타 데이터는 기업, 규정 또는 기타 해당 조항에 따라 기록됩니다. 예를 들어, 해당 조항에 따른 필수 필드는 변경 관리 추적 애플리케이션의 변경 레코드에 나타납니다. • **효율성**—적용된 투입 수준에서 최저의 투입으로 최대의 결과물을 생성할 수 있습니다. • **효과성**—원하는 결과물 또는 목적을 달성합니다.
2007.2.3	경영진은 감사 주제 및 관련 의견 표명을 정의하고 승인하는 일을 담당합니다. 감사 실무자들은 경영진이 수립한 의견 표명이 다른 표준에 대한 권위 있는 성명과 비교해서 박식한 독자 또는 사용자가 기대하는 수준임을 보장해야 합니다.

2007.2.4	감사 실무자들이 감사 업무를 수락하기 위한 전제조건은 감사 감사 주제와 의견 표명에 대한 모든 필수 정보를 감사 실무자들에게 제공하는 책임을 완전히 이해하고 있다는 것을 경영진으로부터 확인받는 것입니다. 감사 실무자들이 경영진이 이 책임을 이행할 수 없다고 생각되면 다음과 같이 해야 합니다. ● 감사 실무자들은 IT 감사 및 보증 관리진 및 감사 기능의 거버넌스 책임자들에게 식별된 문제를 알려야 합니다. ● 제안된 감사 업무를 수락하지 않거나 업무와 연관된 위험 수준에 따라 적절한 행동 방침을 결정하십시오.
2007.2.5	감사 실무자들은 감사 업무에 대해 선택한 의견 표명을 검토하고 이들이 어떠한지 확인해야 합니다. ● **충분성**—감사 업무의 목적을 충족하기에 충분함. 감사 범위의 감사 주제에 대한 의견이나 결론을 표현해야 합니다. ● **유효성**—감사 범위의 감사 주제가 제공될 때, 테스트할 수 있음 ● **관련성**—감사 범위의 감사 주제에 직접 관련되고 감사 업무의 목적을 충족하기에 유용함

2007.3 감사 주제 기준

2007.3.1	감사 실무자들은 미리 결정된 기준을 통하여 감사 업무의 감사 주제를 평가하여, 감사 주제에 대한 의견이나 결론을 나타내야 합니다. 감사 실무자들은 관련 의견 표명을 보증하도록 하는 기준을 평가해야 합니다.
2007.3.2	한 기준이 여러 의견 표명에 연결될 수 있습니다. 또한 한 의견 표명이 여러 기준에 의해 지지 받을 수 있습니다. 이러한 모든 것은 그 의견 표명 달성을 보증하는 것에 기여할 수 있습니다.
2007.3.3	감사 실무자들이 기준이 모든 관련 의견 표명을 완전히 지지하지 않는다고 결론 내릴 경우, 이들은 기존 기준을 변경하거나 내용을 추가할 것을 권고해야 합니다. IT 감사 및 보증 관리진은 새 기준이나 수정된 기준을 검토하고 승인하거나 거부해야 합니다.
2007.3.4	감사 실무자들은 기준이 완전히 관련 의견 표명을 지지한다고 평가한 후, 기준이 객관적이고 측정 가능한 분석의 대상일 수 있는지 여부를 평가해야 합니다.

2007.4 제3자가 제시한 의견 표명

2007.4.1	제3자에게 운영 업무를 아웃소싱하는 기업은 외주된 운영 업무의 통제 환경에 대한 보고서를 받습니다. IT 감사 및 보증이 감사업무를 지원하기 위하여, 외주된 운영 부문과 관련된 보고서에 의존하여야 하는 경우, 감사 실무자들은 각 보고서를 검토하여 다음 사항에 대한 여부를 확인해야 합니다. ● 보고서가 관련 있는 독립 전문가 기구에서 발행되었는지 여부. ● 감사 의견이 한정 의견인지 적정 의견인지 여부. ● 통제 목적의 범위가 기업에서 요구한 통제를 적절하게 다루는지 여부. ● 감사 수행 기간이 기업 기대와 일치하는지 여부. ● (보고서의 전체 적격성을 이끌어내지 못한) 특정 통제 결함이 기업과 관련 있는지 여부. ● 사용 중인 의견 표명이 필수 의견 표명과 일치하는지 여부. IT 감사 및 보증 관리진은 어떤 분석이 수행되고 어떤 결론에 도달했는지 문서화해야 합니다. 감사 실무자들은 범위에 외주된 운영이 있는 감사 업무의 일환으로, 경영진의 의견 표명을 확인하고 공식적으로 승인하도록 해야 합니다.
2007.4.2	또한 기업은 컨설턴트 또는 외부 감사자와 같은 제삼자에게서 보고서를 받을 수 있습니다.

2007.5 결론 및 보고서

2007.5.1	감사 실무자들은 기준에 맞추어 감사 업무의 감사 주제를 평가한 후, 관련 기준에 대한 발견사항의 집계를 바탕으로, 전문가적 판단으로 각 의견 표명에 대한 결론을 내야 합니다.
2007.5.2	결론을 내린 후, 감사 실무자들은 감사 주제에 대한 간접적 또는 직접적 보고서를 발행해야 합니다. ● **간접적인 보고서**—감사 주제에 대한 의견 표명에 대해(예: 감사 주제의 구성요소에 대한 "완전성" 의견 표명에 대해): "효과성 테스트를 바탕으로, 우리는 선택한 기준에 따라 중요한 모든 측면에서 운영으로 이관된 IT 시스템 변경 사항이 변경 관리 추적 애플리케이션에서 완전히 기록되었다고 판단합니다." ● **직접적인 보고서**—감사 주제 자체에 대해(예: 전체 감사 주제에 대해): "운영 중인 효과성 테스트를 바탕으로, 우리는 선택한 기준에 따라 모든 자료 측면에서 IT 시스템 변경 사항이 필수 변경 관리 추적 절차를 따르고 있다고 봅니다."

2007.6 기타 고려사항

2007.6.1	IT 감사 및 보증 감사 실무자는 다음을 고려해야 합니다. ● 감사 주제 평가의 바탕이 되는 기준을 평가하여 이것이 의견 표명을 뒷받침하도록 해야 합니다. ● 의견 표명이 감사 대상이 될 수 있는지와 입증된 정보에 의해 뒷받침되는지 여부를 파악해야 합니다. ● 의견 표명이 적합하게 결정된 기준을 바탕으로 하는지와 객관적 및 측정 가능한 분석의 대상인지 여부를 파악해야 합니다. ● 권위 있는 공표의 다른 표준과 비교하여, 경영진이 수립한 의견 표명이 올바르다는 합리적 기대를 충족하기에 충분함을 확인해야 합니다. ● 기업을 대표하여 통제를 수행하는 제 삼자에 의해 수립된 의견 표명이 경영진에 의해 확인되고, 받아들여 지는지 확인해야 합니다. ● 감사 주제에 대해 직접 보고하거나(직접 보고) 감사 주제에 관한 의견 표명에 대해 보고(간접 보고)해야 합니다. ● 전문가적 판단과 함께 기준에 대한 종합적인 발견사항을 바탕으로 각 의견 표명에 관한 결론을 수립해야 합니다.

표준 1007 및 지침 2007을 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM01 거버넌스 프레임워크 설정 및 유지보수 보장	기업 거버넌스 접근방식에 통합되고 조정되어, 일관된 접근방식을 제공합니다. I&T 관련 결정은 기업의 전략 및 목적에 따라 이루어지고 원하는 가치가 실현됩니다. 이를 위해, I&T 관련 프로세스가 효과적이고 투명하게 감독되고, 법적, 계약적, 규제적 요구사항을 준수하는지, 그리고 이사회 구성원에 대한 거버넌스 요구사항이 충족되는지 확인합니다.
EDM02 이익 제공 보장	I&T 사용 지원 추진 전략, 서비스 및 자산에서의 최적의 보안 가치, 솔루션 및 서비스의 비용 효율적인 제공, 그리고 비즈니스 요구가 효과적이고 효율적으로 지원되는 비용 및 가능한 편익에 대한 신뢰할 수 있고 정확한 그림.
EDM03 위험 최적화에 대한 보장	I&T 관련 기업 위험이 기업의 위험 수용범위 및 위험감수도를 초과하지 않고, 기업 가치에 대한 I&T 위험의 영향이 식별되고 관리되고, 규정 준수 실패 가능성이 최소화되도록 합니다.
EDM04 자원 최적화 보장	기업의 자원 요구가 최적의 방식으로 충족되고, I&T 비용이 최적화되고, 이익 실현 가능성이 높아지고 미래 변화에 대비되도록 해야 합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

일반 표준 1008: 기준

내용	**1008.1** IT 감사 및 보증 실무자는 감사 주제가 평가될 때 바탕이 되는 객관적이고, 완전하며, 적절하고, 신뢰할 만하고, 측정 가능하고, 이해 가능하며, 널리 인식되고, 권한이 있고, 보고서의 모든 독자 및 사용자가 이해할 수 있고 이들이 이용할 수 있는 기준을 선택해야 합니다.
	1008.2 IT 감사 및 보증 실무자는 기준의 수용 가능성을 고려하고 인식되고 권위 있으며 공개적으로 사용할 수 있는 기준에 중점을 두어야 합니다.

일반 지침 2008: 기준

2008.1 소개 이 지침의 목적은 IT 감사 및 보증 실무자가 관련 출처에서 제공되는 기준 중 감사 주제가 평가될 적합하고, 수용 가능한 기준을 선택하는 과정을 지원하기 위한 것입니다. 지침 내용 섹션은 다음과 같은 주요 감사 및 보증 감사 주제에 대한 정보를 제공하도록 구성되었습니다.

2008.2 기준 선택 및 사용

2008.3 적합성

2008.4 수용 가능성

2008.5 출처

2008.6 감사 업무 중 기준 변경

2008.2 기준 선택 및 사용

2008.2.1	감사 실무자들은 감사 주제가 평가될 기준을 선택해야 합니다. 기준을 선택할 때, 감사 실무자들은 기준의 적합성, 수용 가능성 및 출처를 신중하게 고려해야 합니다.
2008.2.2	감사 실무자들은 신중하게 기준 선택을 고려해야 합니다. 지역 법과 규정을 준수하는 것이 중요하며 필수 요건으로 고려되어야 합니다. 그러나, 많은 감사 업무에는 법이나 규정이 적용되지 않는 변경 관리, IT 일반 통제 및 접근 통제와 같은 영역이 포함됩니다. 이에 더하여, 카드 결제 업계 등 일부 업계에서는 필수 의무 요건을 두고 있습니다. 지역 및 국제 데이터 보호 규칙과 개인정보 보호 및 보안 규정의 관련성을 고려해야 합니다. 입법상 요건이 규범적이지 않으면, 감사 실무자들은 선택한 기준이 감사 목적을 충족하여 제정법을 준수함을 보장해야 합니다.
2008.2.3	감사 주제를 일관되게 평가하려면 적합하고 수용 가능한 기준을 사용해야 합니다. 그렇지 않으면, 도출된 결론이나 의견이 독자에 의해 잘못 이해되거나 잘못 해석될 여지가 있습니다.
2008.2.4	감사 실무자들은 개인의 기대, 경험 또는 판단을 근거로 감사 주제를 평가하지 않아야 합니다.
2008.2.5	기준을 쉽게 사용할 수 없거나, 기준이 불완전하거나 해석의 대상인 경우, 감사 실무자들은 기준에 대한 설명과 보고서가 공정하고, 객관적이고, 이해할 수 있도록 하는 데 필요한 다른 정보를 보고서에 포함해야 합니다.
2008.2.6	기준 사용으로 독자나 사용자를 호도하지 않는 공정하고 객관적인 의견 또는 결론이 수립되도록 하려면 전문가적 판단을 사용해야 합니다. 경영진이 전체 요건을 모두 충족하는 기준을 수립하지 않을 수도 있습니다.

2008.3 적합성

2008.3.1	감사 실무자들은 감사 주제를 평가하는데 사용된 기준의 적합성 및 타당성을 평가해야 합니다. “국내법은 데이터 트랜잭션 수행 시 고객의 모든 개인정보는 항상 비공개로 유지되어야 한다고 규정합니다”라는 예시 기준은 다음 기준 속성을 명확히 하는데 사용됩니다. • **객관성**—감사 실무자들의 발견사항과 결론에 부정적인 영향을 미칠 수 있고, 그로 인해 감사 보고서의 사용자를 호도할 수 있는 편견이 없습니다(예를 들어, 기준이 국내법에서 비준되었기 때문에 객관적입니다). • **완전성**—감사 주제에 관한 실무자의 결론에 영향을 줄 수 있는 모든 기준이 감사 업무 수행시 식별되고 사용되도록 충분히 완전합니다. 따라서, 감사 업무의 목표를 고려할 때 사용된 모든 기준의 완전성을 달성해야 합니다. • **관련성**—감사 주제와 관련 있고 감사 업무의 목적을 충족시키는 발견사항 및 결론에 기여합니다. 기준은 상황에 따라 다를 수 있습니다. 동일한 감사 주제에 대해서도 감사 업무의 목적 및 상황에 따라 다른 기준이 있을 수 있습니다. 예를 들면, 데이터 트랜잭션이 감사 업무의 범위에 있으므로 기준은 관련성이 있다고 간주됩니다. • **신뢰성**—유사한 상황에서 다른 감사 실무자가 적용할 때 기준은 기본 감사 주제를 합리적인 방식으로 일관되게 측정하거나 평가하고 일관된 결론을 도출해 낼 수 있도록 해야 합니다. • **측정 가능성**—유사한 상황에서 다른 감사 실무자들이 적용할 때 감사 주제를 일관되게 측정하고 일관된 결론을 도출할 수 있도록 합니다. 예를 들면, 보호되지 않은 개인 정보와의 모든 데이터 트랜잭션은 고유하게 식별되어 일관되게 측정될 수 있습니다. • **이해 용이성**—명확하게 전달되고 대상자가 상당히 다른 해석을 해선 안 됩니다. 예를 들어, 법의 이 조항이 이미 복수의 법원 판결의 대상이 되어, 법의 실질적인 집행과 해석에 대한 명확한 이해를 확립하는데 도움을 주므로, 기준은 이해하기 쉽습니다.

2008.4 수용 가능성

2008.4.1	사용자가 보증 활동의 기본과 발견 사항 및 결론의 관련성을 이해할 수 있도록, 기준의 수용 가능성은 감사 보고서의 사용자에 대한 기준의 가용성에 의해 영향을 받습니다. 수용 가능한 기준은 다음과 같은 특성이 포함될 수 있습니다. • **인정**– 대상자가 충분히 인정하여 사용에 대한 문제가 제기되지 않습니다. • **권위 있음**–지역 내에서 권위 있는 의견 표명을 반영하는 것은 감사 주제에 적합합니다. 예를 들면, 권위 있는 의견 표명은 전문가 기구, 산업 그룹, 정부 및 규제기관에서 나올 수 있습니다. • **공개적으로 사용 가능**–ISACA, 국제 회계사 협회(IFAC), 기타 인정되는 정부, 법무 또는 전문가 기구 등 전문 회계 및 감사 기구가 수립한 표준이 해당됩니다. • **전체 사용자 이용성**–기준이 대중적으로 이용 가능하지 않은 경우, 기준은 감사 보고서의 일부를 형성하는 의견 표명을 통해 전체 사용자에게 전달되어야 합니다. 표명은 감사가 가능하도록 "적합한 기준" 요건이 만족되는 감사 주제에 관한 진술서로 구성됩니다.
2008.4.2	실무자들은 감사 업무에 사용된 기준이 다음 중 무엇인지 확인해야 합니다. • **대외적으로 인정됨**–인정되고 권위 있으며 공개적으로 사용 가능하거나 • **대외적으로 확인됨**–특정 감사 업무를 위해 경영진진이 개발한 기준은 인정되고 권위 있으며 공개 적으로 사용 가능하다고 간주되지 않습니다. 경영진이 바라는 감사 업무의 결과를 암묵적으로 강요하지 않는다는 것을 확인하기 위하여, 이러한 기준은 사용 전에, 인정받는 독립적인 제3자가 외부 검증을 해야합니다.

2008.5 출처

2008.5.1	실무자들은 IT 보증 기준의 적합성과 가용성을 고려할 뿐만 아니라, 사용 측면 및 잠재적 고객 측면에서 기준의 출처도 고려해야 합니다. 예를 들어, 감사 주제에 정부 규제가 포함될 경우 감사 주제에 적용되는 법률 및 규정으로부터 수립된 의견 표명에 기초한 기준이 가장 적합한 선택입니다. 다른 경우에는, 업계 또는 무역 협회 기준이 적합할 수 있습니다. 고려할 순서로 나열된, 사용 가능한 기준의 출처는 다음과 같습니다. • **ISACA가 제정한 기준**–이 기준은 대중적으로 이용 가능한 기준 및 표준으로서, IT 감사, 위험, 개인정보 보호, 거버넌스 및 보안에서 인정 받는 국제 전문가에 의해 동료 검토, 철저한 실사 절차를 거쳤습니다. • **다른 전문가 기구에 의해 수립된 기준**–ISACA 표준 및 기준과 유사하게, 이 기준은 감사 주제와 관련이 있고, 다양한 분야의 전문가에 의해 수립되며, 동료 검토, 철저한 실사 절차를 거칩니다. • **법률 및 규정에 의해 수립된 기준**–법률과 규정이 기준의 근거가 될 수 있으나, 적용 시에는 주의를 기울여야 합니다. 종종 표현 문구들이 복잡하고 특정한 법적 의미를 내포하고 있습니다. 많은 경우, 요구사항을 의견 표명으로 재명시해야 할 수도 있습니다. 또한, 일반적으로 법률에 관한 의견을 개진하는 것은 법률 전문가로 제한되어 있습니다. • **공정한 프로세스를 준수하지 않은 기업이 수립한 기준**–여기에는 공정한 프로세스를 준수하지 않아 공개적 자문 및 논쟁의 대상이 되지 않았던 법인에 의해 수립된 관련 기준이 포함됩니다. • **감사 업무를 위해 특별히 수립된 기준**–감사 업무를 위해 특별히 수립된 기준이 적절할 수 있지만, 실무자들은 기준이 적합하도록(특히 객관적이고, 완전하며, 측정 가능하도록) 각별히 주의를 기울여야 합니다. 감사 업무를 위해 특별히 수립된 기준은 의견 표명의 형태를 띱니다. 일반적으로 이러한 기준에는 특정 사용자가 필요합니다. 예를 들어, 내부 통제 시스템의 효과성을 평가하기 위해 수립된 기준으로 다양한 프레임워크를 사용할 수 있습니다. 그러나, 특정 사용자는 특정 요구를 충족하는 일련의 기준을 수립할 수 있습니다(예 : 권한이 부여된 승인 계층구조). 실무자들은 감사 보고서에 특정 기준이 해당 감사 업무에 한정된다는 점을 명확히 명시해야 합니다. 이들은 수립된 기준이 의도된 사용자를 호도할 수 있는지 여부를 고려하고, 필요한 경우 기준에 대한 더 많은 정보를 제공해야 합니다. 경영진이 기준을 수립한 경우, 외부의 확인을 받고 보고서에 명시해야 합니다.

2008.6 감사 업무 중 기준 변경

2008.6.1	감사가 진행됨에 따라, 감사 주제에 대한 추가 정보 및 통찰력에 의해 선택한 기준이 변경될 수 있습니다. • 감사 목적을 달성하기 위해 특정 기준이 더 이상 필요하지 않을 수 있으므로, 이후에는 기준과 관련된 추가적인 감사 업무가 필요 없습니다. • 감사 목적을 달성하기 위해 별도의 기준이 필요할 경우, 실무자들은 기준을 선정하고 관련된 감사 업무을 실시합니다.

기준 1008 및 지침 2008을 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM01 거버넌스 프레임워크 설정 및 유지보수 보장	기업 거버넌스 접근방식에 통합되고 조정되어, 일관된 접근방식을 제공합니다. I&T 관련 결정은 기업의 전략 및 목적에 따라 이루어지고 원하는 가치가 실현됩니다. 이를 위해, I&T 관련 프로세스가 효과적이고 투명하게 감독되고, 법적, 계약적, 규제적 요구사항을 준수하는지, 그리고 이사회 구성원에 대한 거버넌스 요구사항이 충족되는지 확인합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

수행 기준

수행 기준 1201: 계획 수립 시 위험 평가

내용	**1201.1** IT 감사 및 보증 담당자는 적절한 위험 전반적인 IT 감사계획을 수립하고, IT 감사자원의 효과적인 할당을 위한 우선선위를 결정하기 위하여, 적절한 위험평가 접근방식 (즉, 정량적 및 정성적 요인을 모두 포함한 데이터 기반 접근방법)과 지원 방법론을 사용해야 합니다.
	1201.2 IT 감사 및 보증 실무자는 개별 업무를 계획할 때 검토 대상 영역과 관련된 위험을 식별하고 평가해야 합니다.
	1201.3 IT 감사 및 보증 실무자는 감사 업무를 계획할 때 해당 감사 주제의 위험, 감사 위험 및 기업에 대한 관련 노출을 고려해야 합니다.

수행 지침 2201: 계획 수립 시 위험 평가

2201.1 소개 이 지침의 목적은 IT 환경에서 위험과 위협을 식별하는 데 도움을 주는 것입니다. 지침은 다음을 개발하기 위한 위험 평가 접근방식을 적용하는 과정을 안내합니다.

- 모든 연간 감사 업무를 포괄하는 IT 감사 계획
- 개별 감사 업무에 중점을 두는 감사 업무 프로젝트 계획

지침은 IT 감사 및 보증 실무자들이 직면하는 다양한 위험의 세부사항을 제공합니다. 지침 내용 섹션은 다음과 같은 주요 감사 및 보증 감사 주제에 대한 정보를 제공하도록 구성되었습니다.

2201.2 IT 감사 계획의 위험 평가

2201.3 위험 평가 방법론

2201.4 개별 업무의 위험 평가

2201.5 감사 위험

2201.6 고유 위험

2201.7 통제 위험

2201.8 적발 위험

2201.9 기타 고려사항

2201.2 IT 감사 계획의 위험 평가

2201.2.1	위험 평가는 감사 계획 프로세스 중 수행되어야 하며, 변화하는 비즈니스 조건과 새롭게 부상하는 위험에 기반하여 사전에 수정되어야 합니다. 실무자들은 조직의 전략적 계획과 목표 및 기업의 위험 관리 프레임워크 및 계획을 고려해야 합니다. 이것은 IT 감사 일정의 개발 프로세스를 용이하게 합니다.
2201.2.2	IT 감사 영역의 전체 범위와 관련된 위험을 정확하고 완전하게 평가하려면 실무자들은 IT 감사 일정을 세울 때 다음 요소를 고려해야 합니다. • 가능한 모든 감사 활동의 범위를 포괄하고 시스템, 애플리케이션 및 프로세스의 중요도를 고려하여, IT 감사범위 내 모든 영역에 적용. • 경영진이 제공한 위험 평가의 신뢰성 및 적합성 • 발생 가능한 위험 또는 문제를 감독, 조사 및 보고하기 위한 경영진의 프로세스 • 검토 중인 활동과 관련된 위험 대응
2201.2.3	적용된 위험 평가 접근방식은 IT 감사 및 보증 작업의 우선순위 지정 및 스케줄링 프로세스에 도움을 주어야 합니다. 이것은 감사 관심 영역과 항목을 선택할 때도 지원해야 합니다. 이것은 특정 IT 감사 업무를 계획하고 시행하기 위한 의사 결정 프로세스를 안내해야 합니다.
2201.2.4	실무자들은 적용된 위험 평가 접근방식이 거버넌스 책임자에 의해 승인되고 다양한 업무 이해관계자에게 배포되는지 확인해야 합니다.
2201.2.5	실무자들은 IT 감사 계획을 완료하고 특정 업무에 대한 요구사항을 충족하는 데 필요한 IT 감사 자원을 수량화하고 정당화하기 위해 위험 평가를 사용해야 합니다.
2201.2.6	위험 평가를 기반으로, 실무자들은 IT 감사 및 보증 활동에 대한 프레임워크 역할을 하는 IT 감사 일정을 수립해야 합니다. 이 일정의 조건은 다음과 같습니다. • 비 IT 감사 및 보증 요구사항 및 활동을 고려해야 합니다. • 적어도 매년 업데이트되어야 합니다. • 거버넌스 책임자에 의해 승인되어야 합니다. • 감사 헌장에 설정된 책임에 대응해야 합니다.
2201.2.7	전반적인 IT 감사 계획을 수립할 때, 적절한 위험 평가 접근방식을 따라야 합니다. 위험 평가의 목표는 더 집중적으로 감사해야 하는 활동을 식별하고 부정확한 결론에 도달할 위험을 줄이는 것입니다.

2201.3 위험 평가 방법론

2201.3.1	실무자들은 IT 감사 일정상 감사 업무가 완벽하고 정확하게 수행되도록 하는 적절한 위험 평가 방법론을 고려해야 합니다.
2201.3.2	실무자들은 방법론에 적어도 시스템 가용성, 데이터 무결성 및 비즈니스 정보 기밀성과 관련하여 기업이 처하는 위험에 대한 분석을 방법론에 포함시켜야 합니다.
2201.3.3	위험 평가 프로세스를 지원하기 위해 많은 위험 평가 방법론을 사용할 수 있습니다. 이러한 방법론들은 실무자의 판단에 따른 고, 중, 저의 단순한 분류에서부터 숫자로 위험 평가를 하는 더 정량적이고 과학적인 계산에 이르기까지 다양합니다. 두 가지가 결합된 조합인 다른 방법론도 있습니다. 실무자들은 감사 대상 기업이나 또는 주제에 적합한 복잡도와 상세정보를 고려해야 합니다. 위험 평가 수행에 대한 구체적인 지침은 ISACA 간행물, 위험 IT 프레임워크및 위험 IT 실무자 안내서에서 찾을 수 있습니다.
2201.3.4	모든 위험 평가 방법론은 프로세스의 특정 시점(예: 다양한 매개변수에 가중치를 할당할 경우)에서 주관적인 판단에 의존합니다. 실무자들은 특정 방법론을 사용할 때 필요한 주관적인 결정사항을 식별하고 적절한 수준의 정확성과 합리성으로 판단하고 그 판단을 검증할 수 있는지 여부를 고려해야 합니다.

2201.3.5	가장 적절한 위험 평가 방법론을 결정하기 위해 실무자들은 다음 사항을 고려해야 합니다. • 수집해야 하는 정보의 유형. 일부 시스템은 재무적 효과를 유일한 측정 수단으로 사용합니다. 이것이 IT 감사 업무에 항상 적합하지는 않습니다. • 방법론을 사용하는데 필요한 소프트웨어 또는 기타 라이센스 비용 • 필요한 정보를 이미 사용할 수 있는 범위 • 신뢰할 수 있는 산출물을 얻기 전에 먼저 수집해야 하는 추가 정보량 및 정보 수집 비용(수집 과정에서 필요한 시간 투자 포함) • 방법론에 대한 다른 사용자들의 의견과 감사 효율성 및 효과성을 향상시키는데 이 방법론이 얼마나 도움이 되었는지에 대한 그들의 견해 • 수행된 감사 작업의 유형과 수준을 판별하기 위한 수단으로 방법론을 수락하겠다는 IT 감사 영역의 거버넌스 책임자의 의지
2201.3.6	모든 상황에 적합할 것으로 기대할 수 있는 단일 위험 평가 방법론은 없습니다. 위험, 위협, 취약성, 위험 선호도 및 위험 한도는 바뀔 수 있으므로, 실무자들은 선택한 위험 평가 방법론의 적합성을 주기적으로 재평가해야 합니다.
2201.3.7	실무자들은 선택한 위험 평가 기법을 사용하여 전체 IT 감사 일정을 수립하고 특정 감사 업무를 계획해야 합니다. 다음과 같은 결정사항을 계획할 때 다른 감사 기법과 함께 위험 평가를 고려해야 합니다. • 감사 대상 영역 또는 비즈니스 기능 • 감사에 할당될 시간과 자원의 양 • 감사 절차의 성격, 범위 및 시기
2201.3.8	채택된 위험 평가 방법론은 일관되고, 유효하고, 비교 가능하며, 반복 가능한 결과를 생성해야 하고, 경영진의 합의를 얻어야 합니다. 방법론에 의해 생성된 위험 평가는 (일정 기간) 일관되고, 유효하고, (동일한 평가 방법론을 사용하는 이전/이후 평가와) 비교 가능하고, 반복 가능(유사한 일련의 사실을 제공할 때, 동일한 평가 방법론을 사용하면 유사한 결과가 생성됨)해야 합니다.

2201.4 개별 업무의 위험 평가

2201.4.1	개별 업무를 계획할 때, 실무자들은 검토 중인 영역과 관련된 위험을 식별하고 평가해야 합니다. 위험 평가 결과는 감사 업무 목적에 반영되어야 합니다. 위험 평가 중, 실무자들은 다음 사항을 고려해야 합니다. • 이전 감사 업무의 결과, 검토 및 발견사항(교정 활동 포함) • 기업 위험 평가 프로세스 • 특정 위험의 발생 가능성 • 특정 위험이 발생할 경우 그 위험의 영향(금전적 또는 기타 가치 측정)
2201.4.2	실무자들은 위험을 평가하기 전에 감사 범위 내의 활동에 대해 완전히 이해하고 있어야 합니다. 그들은 이해관계자 및 기타 당사자들로부터 의견과 제안사항을 요청해야 합니다. 감사 위험에서 발생 가능한 위험을 올바르게 판별하고 관련 영향을 살펴보려면 충분한 이해가 필요합니다.
2201.4.3	특정 IT 감사 및 보증 절차를 계획할 때, 실무자들은 중요성 임계치가 낮을수록 감사 기대가 정밀해지고 감사 위험이 커진다는 점을 인식해야 합니다.
2201.4.4	특정 IT 감사 및 보증 절차를 계획할 때, 실무자들은 기존 절차의 성격, 시기 또는 범위 수정을 요구할 수 있는 발생 가능한 불법 행위와 잠재적 소송을 지원하는데 필요한 해당 문서를 고려해야 합니다.
2201.4.5	감사 위험이 높거나 중요성 임계치가 낮은 상황에서 추가적인 보증을 얻기 위해, 실무자들은 IT 감사 테스트의 범위 또는 성격을 확장하거나 실증 테스트를 증가하거나 확대해야 합니다.

2201.5 감사 위험

2201.5.1	감사 위험은 감사 결과를 바탕으로 부정확한 결론에 도달할 수 있는 위험을 나타냅니다. 감사 위험의 3가지 요소: ● 고유 위험 ● 통제 위험 ● 적발 위험
2201.5.2	실무자들은 각 위험 요소를 고려하여 전체 위험도를 판별해야 합니다. 감사 위험은 고유 위험과 통제 위험을 포함하는 감사 주제와 적발 위험으로 구성됩니다.

2201.6 고유 위험

2201.6.1	고유 위험은 관련 내부 통제가 없다고 가정할 때, 중요할 수 있는 오류(개별적으로 또는 다른 오류와 함께)에 대한 감사 영역의 민감성입니다. 예를 들어, 운영체제 보안 약점을 통해 데이터 또는 프로그램이 변경되거나 노출되면 잘못된 관리 정보 또는 경쟁적 불이익을 초래할 수 있으므로, 적절한 통제가 없는 운영체제와 관련된 고유 위험은 대개 높습니다. 반대로, 적절한 분석에 의해 통제가 없는 독립형 PC가 비즈니스에서 중요한 목적에 사용되지 않는다고 보여질 때, 이 PC에 대한 보안과 관련된 고유 위험은 보통 낮습니다.
2201.6.2	IT 감사자는 테스트될 영역의 범위가 주요 비즈니스 시스템에 영향을 준다고 간주하므로, 고유 위험이 높을 것으로 예상됩니다.

2201.7 통제 위험

2201.7.1	통제 위험은 감사 영역에서 일어날 수 있고 개별적으로 또는 다른 오류와 함께 중요할 수 있는 오류가 내부 통제 시스템에서 적시에 방지되거나 탐지되고 수정되지 않는 위험입니다. 예를 들어, 로깅된 정보가 많으면 실수로 인한 이상징후를 식별하지 못하는 사고가 발생할 수 있으므로, 컴퓨터 로그의 수동 검토와 관련된 통제 위험이 높을 수 있습니다. 프로세스는 일관되게 적용되므로 전산화된 데이터 검증 절차와 연관된 통제 위험은 대개 낮습니다.
2201.7.2	감사 실무자들이 통제 위험을 높게 평가해야 하는 경우: ● 관련 내부 통제가 식별되지 않는 경우 ● 관련 내부 통제가 테스트(즉, 수행과 설계 비교)를 통해 검증되고 효과적으로 작동한다고 입증되지 않는 경우
2201.7.3	실무자들은 곳곳에 전반적이고 상세한 IT 통제를 모두 고려해야 합니다. ● 전반적 IT 통제는 일반 통제의 하위 집합이며, IT 환경의 관리 및 모니터링에 중점을 두는 면에서 일반 통제입니다. 이들은 모두 IT 관련 활동에 영향을 줍니다. 실무자의 작업에 미치는 전반적 IT 통제의 영향은 비즈니스 프로세스 시스템에서 응용 통제의 신뢰성으로 제한되지 않습니다. 또한 전반적 IT 통제는 애플리케이션 프로그램 개발, 시스템 구현, 보안 관리 및 백업 절차 등에 대한 세부 IT 통제의 신뢰성에 영향을 줍니다. 전반적 IT 통제가 약해서 IT 환경의 관리 및 모니터링이 잘 되지 않을 경우, 상세 수준에서 작동하도록 설계된 통제가 비효과적일 수 있다는 높은 위험의 가능성을 경고해야 합니다. ● 세부 IT 통제는 전반적 IT 통제에 포함되지 않은 일반 통제와 응용 통제로 구성됩니다. COBIT 2019 프레임워크에 따라, 세부 IT 통제는 정보 및 기술의 거버넌스 및 관리와 관련이 있습니다.
2201.7.4	실무자들은 전반적 IT 통제의 부적절성으로 인해 세부 IT 통제의 제한사항 및 단점이 발생할 수 있는 위험을 고려해야 합니다.

2201.8 적발 위험

2201.8.1	적발 위험은 실무자의 실증 절차상 중요할 수 있는 오류가 개별적 또는 다른 오류와 결합되어 적발되지 않는 위험입니다. 예를 들어, 감사 전체 기간 동안 로그를 감사 시 사용하지 못할 수 있으므로, 종종 애플리케이션 시스템에서 보안 위반 식별과 연관된 적발 위험이 높습니다. 재난 복구 계획이 없음을 식별하는 것과 관련된 적발 위험은 그 존재 여부가 쉽게 확인되므로, 낮은 경향이 있습니다.
2201.8.2	필요한 실증 테스트 수준을 판별할 때, 실무자들은 다음 사항을 고려해야 합니다. ● 고유 위험 진단 평가 ● 준거성 테스트 후 통제 위험에 대한 결론
2201.8.3	고유 및 통제 위험의 진단평가가 결과가 높을수록, 일반적으로 실무자들은 실증 감사 절차 수행에서 더 많은 감사 증거를 얻어야 합니다.

2201.9 기타 고려사항

2201.9.1	지속적인 활동을 계획할 때, IT 감사 및 보증 담당자는 다음을 고려해야 합니다. ● 적어도 1년에 한 번 위험 평가를 실시하고 문서화하여 IT 감사 계획 수립을 용이하게 해야 합니다. ● 위험 평가에 조직의 전략적 계획과 목표 및 전사 리스크 관리 프레임워크 및 추진 전략을 포함해야 합니다. ● 감사 관심 영역 및 항목 선택을 선택하고, 특정한 IT 감사 및 보증 업무를 설계하고 수행하기 위한 결정에 있어 위험 평가를 사용해야 합니다. 일부 관심 영역과 항목은 실무자의 관리와 지속적인 감사로 지속적으로 모니터링될 수 있습니다. ● 관리진의 위험 평가에 의존할 경우, 해당 평가가 적절한 담당자에 의해 승인되었음을 확인해야 합니다. 위험 평가는 관리진의 위험 수용 사례를 문서화해야 합니다. ● 감사 담당자에 의해 위험 평가가 수행된 경우, 이 위험 평가를 조직 전체 다른 사람(즉, 독립적인 위험 관리 담당자)이 수행한 위험 평가와 비교합니다. 불일치성을 해결합니다(즉, 감사 담당자는 위험을 높게 평가하는 반면, 위험 관리 담당자는 위험을 낮게 평가함). ● 위험 평가를 바탕으로 IT 감사 및 보증 업무의 우선 순위를 정하고 일정을 수립해야 합니다. ● 위험 평가를 바탕으로 다음과 같은 계획서를 수립해야 합니다. ■ IT 감사 및 보증 활동을 위한 프레임워크 역할을 하는 계획서 ■ 비IT 감사 및 보증 요건 및 활동을 고려하는 계획서 ■ 거버넌스 책임자에 의해 1년에 1회 이상 수정 및 승인되는 계획서 ■ 감사 헌장에 설정된 책임을 이행하는 계획서 개별 업무를 계획할 때, IT 감사 및 보증 감사 실무자는 다음을 수행해야 합니다. ● 검토 중인 분야와 관련된 위험을 파악하고 평가해야 합니다. ● 각 업무에 대해 검토 중인 분야와 관련 있는 위험의 예비 평가를 수행해야 합니다. 각각의 구체적인 업무의 목표에는 예비 위험 평가의 결과가 반영되어야 합니다. ● 구체적인 업무의 위험 영역과 관련된 교정 활동을 포함하여, 이전 감사, 검토 및 발견사항을 고려해야 합니다. 위원회의 전체적인 위험 평가 프로세스도 고려해야 합니다. ● IT 감사 계획 및 수행 중에 감사 위험을 적정 수준으로 감소하도록 시도하고, IT 감사 주제 및 관련 통제 장치를 적절하게 평가함으로써 감사 목적을 만족해야 합니다. ● 높은 중요성에 대한 감사 위험을 감소시키기 위해, 통제 테스트를 확대하고(통제 위험 감소) 또는 실증 테스트 절차를 확대하여(적발 위험 감소) 보상함으로써 추가 보증을 확보해야 합니다.

표준 1201 및 지침 2201을 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM01 거버넌스 프레임워크 설정 및 유지보수 보장	기업 거버넌스 접근방식에 통합되고 조정되어, 일관된 접근방식을 제공합니다. I&T 관련 결정은 기업의 전략 및 목적에 따라 이루어지고 원하는 가치가 실현됩니다. 이를 위해, I&T 관련 프로세스가 효과적이고 투명하게 감독되고, 법적, 계약적, 규제적 요구사항을 준수하는지, 그리고 이사회 구성원에 대한 거버넌스 요구사항이 충족되는지 확인합니다.
EDM03 위험 최적화에 대한 보장	I&T 관련 기업 위험이 기업의 위험 수용범위 및 위험한도를 초과하지 않고, 기업 가치에 대한 I&T 위험의 영향이 식별되고 관리되고, 규정 준수 실패 가능성이 최소화되도록 합니다.
APO12 위험 관리	I&T 관련 기업 위험 관리를 전반적인 전사 위험 관리(ERM)와 통합하고 I&T 관련 기업 위험의 비용과 이익을 균형 조절합니다.
MEA03 외부 요건 준수 관리	기업에 적용되는 모든 외부 요건을 준수하도록 합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

수행 표준 1202: 감사 스케줄링

내용	**1202.1** IT 감사 및 보증 담당자는 단기 및 장기간 감사 일정을 만드는 전반적인 전략 계획을 세워야 합니다. 단기 계획은 연내에 수행될 감사로 구성되는 반면, 장기 계획은 미래에 수행될 수 있는 기업의 정보 및 기술(I&T) 환경 내 위험 관련 문제에 기반한 감사로 구성됩니다.
	1202.2 단기간 및 장기간 감사 일정은 모두 거버넌스 및 감독 책임자(예: 감사 위원회)와 합의해야 하고 기업 내에서 알려야 합니다.
	1202.3 IT 감사 및 보증 담당자는 조직의 필요(즉, 예기치 않은 이벤트 또는 계획되지 않은 추진전략)에 대응하도록 단기간 및/또는 장기간 감사 일정을 수정해야 합니다. 예기치 않은 이벤트 또는 예정되지 않은 신규 계획의 감사를 수용하도록 대체된 감사는 추후 다시 할당되어야 합니다.

수행 지침 2202: 감사 스케줄링

2202.1 소개 이 지침은 IT 감사 및 보증 실무자의 감사 스케줄링 과정을 안내합니다.

지침 내용 섹션은 주요 감사 및 보증 업무 주제에 대한 정보를 제공하도록 구조화되었습니다.

2202.2 감사 일정 수립 및 유지보수

2202.3 감사 일정 및 업무 계획

2202.2 감사 일정 수립 및 유지보수

2202.2.1	IT 감사 및 보증 실무자들은 종종 전체 감사 영역으로 칭하는 감사 영역의 인벤토리에 기반한 감사 일정을 수립하고 유지보수해야 합니다. 감사 스케줄링은 감사 헌장에서 식별된 감사 담당자의 책임에 대해 적절한 주의를 기울이도록 하고, 중요한 감사 영역에서 기업의 전략적 목표와 조직의 목적에 대해 적절한 보증이 제공되도록 하는 데 도움을 줍니다.
2202.2.2	장기간 감사 일정은 조직의 요구에 대응하여 주기적으로(적어도 1년에 한 번) 다시 평가해야 합니다. 이 재평가를 통해 감사 담당자는 예기치 않은 중요한 이벤트나 상황에 대응하여 필요할 수 있는 추가 보증 및 감사 업무를 포함할 수 있습니다. 대체된 계획된 감사를 미래 기간에 다시 할당해야 합니다.

2202.3 감사 일정 및 업무 계획

2202.3.1	감사 일정은 잠정적인 감사 시작 날짜, 예비 범위 및 핵심 이해관계자 정보와 함께 기업에 전달될 수 있습니다.

표준 1202 및 지침 2202를 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM01 거버넌스 프레임워크 설정 및 유지보수 보장	기업 거버넌스 접근방식에 통합되고 조정되어, 일관된 접근방식을 제공합니다. I&T 관련 결정은 기업의 전략 및 목적에 따라 이루어지고 원하는 가치가 실현됩니다. 이를 위해, I&T 관련 프로세스가 효과적이고 투명하게 감독되고, 법적, 계약적, 규제적 요구사항을 준수하는지, 그리고 이사회 구성원에 대한 거버넌스 요구사항이 충족되는지 확인합니다.
EDM02 이익 제공 보장	I&T 사용 지원 추진 전략, 서비스 및 자산에서의 최적의 보안 가치, 솔루션 및 서비스의 비용 효율적인 제공, 그리고 비즈니스 요구가 효과적이고 효율적으로 지원되는 비용 및 가능한 편익에 대한 신뢰할 수 있고 정확한 그림.
BAI11 프로젝트 관리	정의된 프로젝트 결과를 실현하고 기업 및 최종 사용자의 참여 및 소통을 개선하여 예기치 않은 지연, 비용 및 가치 하락의 위험을 줄입니다. 프로젝트 산출물의 가치와 품질을 보장하고 정의된 프로그램 및 투자 포트폴리오에 대한 기여를 최대화합니다.

수행 표준 1203: 업무 계획

내용	**1203.1** IT 감사 및 보증 실무자는 수행할 감사 절차의 성격, 타이밍 및 범위를 다루는 각 IT 감사 및 보증 업무를 계획해야 합니다. 계획은 다음 사항을 포함해야 합니다. • 감사 대상 영역 • 목적 • 범위 • 자원(예: 실무진, 도구 및 예산) 및 일정 날짜 • 일정 및 산출물 • 준거법/규정 및 전문 감사 표준 준수 • 법적 또는 규정 준수와 관련되지 않은 업무에 대한 위험 기반 접근방식 사용 • 업무별 이슈 • 문서화 및 보고 요건 • 관련 기술 및 데이터 분석법 사용 • 잠재적 이익에 대한 업무 비용 고려 • IT 감사 업무 수행 중 발생할 수 있는 상황에 대한 알림 및 단계적 확대 프로토콜(예: 핵심 인력의 범위 제한 또는 사용 불가능) 현장 작업 중, 업무 진행에 따라 계획 중 생성된 감사 절차를 수정해야 할 수 있습니다.
	1203.2 IT 감사 및 보증 실무자는 감사를 완료하는 데 사용될 단계별 절차와 지침을 설명하는IT 감사 및 보증 업무 프로그램을 개발하고 문서화해야 합니다.

수행 지침 2203: 업무 계획

2203.1 소개 이 지침은 IT 감사 및 보증 실무자의 업무를 계획하는 과정을 안내합니다. 지침 내용 섹션은 주요 감사 및 보증 업무 주제에 대한 정보를 제공하도록 구조화되었습니다.

2203.2 목적

2203.3 범위 및 비즈니스 지식

2203.4 위험 기반 접근방식

2203.5 감사 업무 프로젝트 계획 및 감사 프로그램 문서화

2203.6 감사 과정의 변경 사항

2203.2 목적

2203.2.1	실무자들은 감사 업무 목적을 정의하고 감사 업무 프로젝트 계획에서 이를 문서화해야 합니다. 기업의 목표, 운영 및 과제에 대한 이해를 확인할 뿐만 아니라, 감사 업무 목적의 문서화를 통해 테스트로 통제가 적절하게 구축되고 효과적으로 운영되고 있음을 보장할 수 있습니다.
2203.2.2	감사 실무자들은 감사 업무의 목적을 고려하는 감사 업무 프로젝트 계획을 수립해야 합니다. 이러한 목적은 자원, 일정 및 산출물 등의 감사 업무에 영향을 줄 수 있습니다.

2203.3 범위 및 비즈니스 지식

2203.3.1	감사 업무를 시작하기 전에 감사 실무자들은 감사 목적을 충족하기에 적합한 방식으로 작업을 계획해야 합니다. 계획 프로세스 과정에서 감사 실무자들은 기업과 기업의 프로세스에 대한 이해를 구해야 합니다. 그럴 경우, 기업의 목표과 관련하여 검토 중인 영역의 중요성을 판별하는데 도움이 됩니다. 감사 실무자들은 감사 목적을 토대로 감사 작업의 범위를 설정해야 합니다.
2203.3.2	예비 평가 과정에서, 실무자들은 감사 업무의 대상이 되는 특정 기업, 기능, 프로세스 또는 데이터에 상당한 영향을 미칠 수 있는 인력, 이벤트, 트랜잭션 및 실무수행 유형을 이해해야 합니다. 기업에 대한 감사자의 지식은 기업이 처한 비즈니스 및 재정적 위험, 기업 시장의 조건, 그리고 기업이 목적을 충족하기 위해 아웃소싱에 의존하는 범위를 포함해야 합니다. 실무자들은 잠재적 문제를 파악하고, 작업의 목적 및 범위를 정하고, 작업을 수행하고, 의식해야 하는 관리진의 조치를 고려하는 데 이 정보를 사용해야 합니다.

2203.4 위험 기반 접근방식

2203.4.1	위험 평가를 수행하여 기업과 기업의 환경(즉, 전략적 목표와 내부 및 외부 의무)을 이해해야 합니다. 이러한 이해를 바탕으로, 감사 실무자들은 검토할 영역과 활동을 식별할 수 있습니다.
2203.4.2	검토 중인 영역과 기업 IT 환경에 대해 식별된 위험의 위험 평가와 우선순위는 필요한 범위까지 수행되어야 합니다.
2203.4.3	계획 프로세스에서, 감사 실무자들은 감사 작업이 감사 목적을 충족하기에 충분하고 감사 자원을 효율적으로 사용하도록 계획 중요성의 수준을 설정해야 합니다. 예를 들어, 기존 시스템 검토에서, 감사 실무자들은 수행될 작업에 대한 감사 업무를 계획할 때 시스템의 다양한 구성요소의 중요성을 평가해야 합니다. 중요성을 판별할 때 정성적 측면과 정량적 측면을 모두 고려해야 합니다.
2203.4.4	감사 업무를 시작하기 전, 그리고 감사 과정 중, 감사 실무자들은 해당 법과 전문가 감사 표준 준수를 고려해야 합니다.
2203.4.5	감사 실무자들이 대규모 감사 수행(예: 과거 재무 정보의 감사) 과정에서 수집되는 정보를 지원하기 위해 통제 절차에 의존할 목적으로 내부 통제를 평가할 때, 이들은 통제를 사전 평가하고 그 평가를 기준으로 감사 업무 프로젝트 계획을 수립해야 합니다.

2203.5 감사 업무 프로젝트 계획 및 감사 프로그램 문서화

2203.5.1	실무자의 작업 서류는 감사 업무 프로젝트 계획을 포함해야 합니다.
2203.5.2	명확한 프로젝트 정의는 프로젝트 효과성과 효율성을 보장하는 중요한 요인입니다. 감사 업무 프로젝트 계획("프로젝트 계획")은 다음과 같은 참조 항목을 포함해야 합니다. ● 감사 대상 영역 ● 계획된 작업 유형 ● 작업의 전체 목적 및 범위 ● 수행할 진상 조사 인터뷰 ● 획득해야할 관련 정보 ● 획득된 정보와 감사 증거로서의 사용을 확인 또는 입증할 절차 ● 일반 주제 항목. 예: ■ 예산 ■ 자원 가용성 및 할당 ■ 일정 날짜 ■ 보고서 유형 ■ 대상자 ■ 산출물 ● 특정 주제 항목. 예: ■ 증거 수집, 테스트 수행, 보고용 정보 준비/요약에 필요한 도구 파악 ■ 현재 실무수행을 평가하는 데 사용될 평가 기준(기업 정책, 절차 또는 프로토콜) ■ 위험 평가 문서화 ■ 보고 요건 및 배포 ■ 사용 가능한 외부 보고서(의존할 수 있는 정보) ■ 필요한 경우, 요청될 보고서. 예: SSAE18(Statement on Standards for Attestation Engagements 18)
2203.5.3	프로젝트 계획은 감사 업무의 일정과 관련된 요건을 포함해야 합니다. 이러한 요소는 합의된 일정 내에서 감사 업무를 수행하기 위한 기간과 다른 완료 날짜를 포함하되, 이에 제한되지는 않습니다. 프로젝트 계획은 각 프로젝트 단계에 대한 예산 지출과 감사팀 자원 할당을 포함해야 합니다.
2203.5.4	감사 실무자들은 감사 업무에 할당된 감사팀 자원이 감사 업무를 성공적으로 완료하기 위한 적합한 기술과 지식 및 경험을 가지도록 해야 합니다. 감사 실무자들은 IT 감사팀원들의 역량에 가장 잘 맞는 역할과 책임을 할당해야 합니다.
2203.5.5	프로젝트 계획은 감사 업무에 연결된 모든 산출물을 나열해야 합니다.
2203.5.6	프로젝트 계획과 프로젝트 계획의 변경 사항은 IT 감사 및 보증 관리자에 의해 승인되어야 합니다.
2203.5.7	IT 감사 및 보증 관리진에 의한 승인 후, 프로젝트 계획의 부분(예: 범위, 일정, 문서 요건, 인터뷰 일정)은 피감인들에게 알려 피감인들이 필요한 문서 및 자원에 접근할 수 있고 이것의 가용성을 보장할 수 있도록 해야 합니다.

2203.6 감사 과정의 변경 사항

2203.6.1	감사 업무 과정에서 필요에 따라 (IT 감사 및 보증 관리진에 의한 적절한 승인과 함께) 감사 업무 프로젝트 계획을 업데이트하고 변경해야 합니다. 일단 감사가 진행될 때 감사인의 주의가 필요한 문제가 발생하는 경우, 감사 실무자들은 해당 문제를 해결할 방법을 결정해야 합니다. 감사 범위를 확대하거나 별도의 평가 일정을 수립하는 방법이나 그 외의 다른 옵션을 고려할 수 있습니다. IT 감사 실무자는 새로 확인된 문제를 토대로 감사 범위 또는 일정의 변경 사항을 즉시 피감인에게 알려야 합니다.
2203.6.2	감사 업무 계획은 지속적이고 반복적인 프로세스입니다. 예기치 않은 이벤트, 조건의 변화 또는 획득한 감사 증거의 결과에 의해, 감사 실무자들은 계획된 미래 감사 절차의 성격, 시기 및 범위를 수정해야 할 수 있습니다. 예를 들어, 새로운 규정이 공표될 때, 즉시 평가를 수행하여 준수 관점에서 기업에 미칠 수 있는 영향을 확인해야 할 수 있습니다.
2203.6.3	감사 계획은 기업에 대한 위험을 암시하는 예기치 않은 이벤트의 가능성을 고려해야 합니다. 따라서, 감사 업무 프로젝트 계획은 위험에 기반하여 감사 및 보증 프로세스 내에서 이러한 이벤트의 우선 순위화를 지원해야 합니다.

2203.7 기타 고려사항

2203.7.1	IT 감사 및 보증 감사 실무자는 다음을 고려해야 합니다. ● 감사 대상인 활동에 대해 이해해야 합니다. 필요한 지식의 범주는 기업의 특성, 환경, 비즈니스 목적, 위험 영역 및 업무 목적에 따라 결정되어야 합니다. ● 정부 또는 업계에서 발행된 법률, 규정, 규칙, 지시, 지침을 통한 감사 주제 지침 또는 지시 사항을 고려해야 합니다. ● 위험 평가를 수행하여 모든 중요 항목에 대해 업무가 적절히 수행될 것이라는 합리적 확신을 제공해야 합니다. 그래야 감사 전략, 중요도, 자원 요건이 수립될 수 있습니다. ● 해당 활동이 일정 및 예산에 부합되도록 적합한 프로젝트 관리 방법을 사용하여 업무 프로젝트 계획을 수립해야 합니다. ● 업무가 감사 기능의 외부 전문가에 대한 의존(코소싱 또는 아웃소싱)과 다른 법인체(외부 감사자 또는 규제기관)에서 이전에 수행한 테스트에 대한 의존을 포함할 경우 필요한 프로토콜을 개발합니다. 프로토콜은 다음 사항을 정의해야 합니다. ■ 다른 사람들의 작업에 대한 의존이 적절한 전략인 상황 ■ 감사 기능에 대한 작업을 수행할 감사 기능의 외부인들의 적격성 초기 평가 및 지속적인 모니터링 ■ 다른 사람들의 작업에 대한 의존으로 인해 업무에서 제외할 수 있는 상황: - 예 1: 감사 중인 e-commerce 시스템의 지불 게이트웨이 프로세스가 이미 PCI-DSS (Payment Card Industry Data Security Standard)를 준수하는 경우, 지불 게이트웨이 프로세스가 이미 다른 프레임워크에서 감사되고 있으므로 감사 담당자는 이 프로세스의 감사를 제외할 수 있습니다. - 예 2: 다른 기관에서 인증한 환경 건강 및 안정(EHS) 프레임워크가 큰 제조 회사에서 적절히 있는 경우, 감사 업무에서 환경 보안 통제를 제외할 수 있습니다.

2203.7.1
(계속)
	• 감사 계획에 다음과 같은 과제별 문제를 포함해야 합니다.
	  ■ 적합한 지식, 기술, 경험을 갖춘 자원을 이용할 수 있는지 여부
	  ■ 증거 수집, 테스트 수행, 보고용 정보 준비/요약에 필요한 도구 파악
	  ■ 사용할 평가 기준
	  ■ 보고 요건 및 배포
	• IT 감사 및 보증 업무의 프로젝트 계획 및 감사 프로그램을 문서화하여 다음 사항을 명확하게 나타내십시오.
	  ■ 목적, 범위 및 시기
	  ■ 자원
	  ■ 역할과 책임
	  ■ 파악된 위험 분야와 업무 계획에 미치는 영향
	  ■ 사용할 도구 및 기법
	  ■ 수행할 진상 조사 인터뷰
	  ■ 획득해야할 관련 정보
	  ■ 획득된 정보와 증거로서의 사용을 확인하거나 입증할 절차
	  ■ 접근 방식, 방법론, 절차, 예상 결과 및 결론에 대한 가정
	• 시기, 가용성, 경영진 및 피감인의 기타 책무 및 요건에 관한 업무의 일정을 최대한 수립해야 합니다.
	• 새로운 위험, 잘못된 가정, 수행된 절차의 결과 등 업무 중 발생한 문제를 해결하도록 IT 감사 또는 보증 업무 과정 중에 감사 프로젝트를 조정해야 합니다.
	• 감사의 계획 후 단계에서 수행 중인 작업이 비즈니스 목적에 맞게 조정되도록 해야 합니다.
	• 내부 업무의 경우:
	  ■ 각각의 내부 IT 감사 및 보증 업무에 대해 별도의 감사 계약서를 준비해야 합니다.
	  ■ 감사 계약서 또는 이와 동등한 것을 사용하여 감사 헌장의 관련 요소를 피감인에게 전달하여 특정 업무의 참여를 명확히 하거나 확인해야 합니다.
	  ■ 피감사자가 내용을 완전히 파악하고 필요 시 개인, 문서, 기타 자원에 대한 적절하게 접근할 수 있도록 계획을 전달해야 합니다.
	• 외부 업무의 경우:
	  ■ 각각의 외부 IT 및 보증 업무에 대해 별도의 감사 계약서를 준비해야 합니다.
	  ■ 각 외부 IT 감사 및 보증 업무에 대한 프로젝트 계획 및 감사 프로그램을 준비해야 합니다. 여기서 최소한 업무의 목적과 범위를 문서화해야 합니다.
	• 각 IT 감사 및 보증 업무의 업무 요건을 충족하는 데 필요한 IT 감사 자원의 양을 수량화하고 정당화해야 합니다.

표준 1203 및 지침 2203을 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM01 거버넌스 프레임워크 설정 및 유지보수 보장	기업 거버넌스 접근방식에 통합되고 조정되어, 일관된 접근방식을 제공합니다. I&T 관련 결정은 기업의 전략 및 목적에 따라 이루어지고 원하는 가치가 실현됩니다. 이를 위해, I&T 관련 프로세스가 효과적이고 투명하게 감독되고, 법적, 계약적, 규제적 요구사항을 준수하는지, 그리고 이사회 구성원에 대한 거버넌스 요구사항이 충족되는지 확인합니다.
EDM02 이익 제공 보장	I&T 사용 지원 추진 전략, 서비스 및 자산에서의 최적의 보안 가치, 솔루션 및 서비스의 비용 효율적인 제공, 그리고 비즈니스 요구가 효과적이고 효율적으로 지원되는 비용 및 가능한 편익에 대한 신뢰할 수 있고 정확한 그림.
EDM03 위험 최적화에 대한 보장	I&T 관련 기업 위험이 기업의 위험 수용범위 및 위험감수도를 초과하지 않고, 기업 가치에 대한 I&T 위험의 영향이 식별되고 관리되고, 규정 준수 실패 가능성이 최소화되도록 합니다.

수행 표준 1204: 수행 및 감독

내용	**1204.1** IT 감사 및 보증 실무자는 식별된 위험을 포함하는 승인된 IT 감사 계획에 따라 합의된 일정 이내에서 작업을 수행해야 합니다.
	1204.2 IT 감사 및 보증 실무자는 감사목적을 달성하고, 해당 분야에 적용되는 전문 감사기준을 충족하여야 하는 것에 대해 감독 책임이 있는 IT 감사 직원들을 감독해야 합니다.
	1204.3 IT 감사 및 보증 실무자는 자신의 지식 과 기술 내에 있는 업무이거나 감사업무 중 기술을 습득할 수 있다는 합리적 기대 또는 다른 사람의 감독하에 업무를 수행할 수 있다는 합리적 기대가 있을 때에만 감사를 수락해야 합니다.
	1204.4 IT 감사 및 보증 실무자는 감사 목적을 달성하기 위한 충분하고 적절한 증거를 확보하고 보존해야 합니다.
	1204.5 IT 감사 및 보증 감사 실무자는 감사 과정을 문서화해야 하고, 감사 발견사항과 결론을 지지하는 감사업무와 감사 증거를 기술해야 합니다.
	1204.6 IT 감사 및 보증 감사 실무자의 발견사항과 결론은 이 증거의 근본원인 분석과 해석에 의해 지지되어야 합니다.
	1204.7 IT 감사 및 보증 감사 실무자는 적절한 감사 의견 또는 결론을 제공하고 필요한 증거가 추가 테스트 절차를 통해 획득되는 감사 범위의 제약 사항을 포함해야 합니다.

수행 지침 2204: 수행 및 감독

2204.1 소개 이 지침은 IT 감사 및 보증 감사 실무자에게 감사 업무를 수행하고 IT 감사팀원을 감독하는 가이드를 제공 합니다. 지침 내용 섹션은 다음과 같은 주요 감사 및 보증 주제에 대한 정보를 제공하도록 구성되었습니다.

2204.2 감사 수행

2204.3 역할과 책임, 지식 및 기술

2204.4 감독

2204.5 증거

2204.6 문서화

2204.7 발견사항

2204.8 기타 고려사항

2204.2 감사 수행

2204.2.1	감사 실무자들은 승인된 IT 감사 계획에 따라 각 감사 업무를 계획하고 수행해야 합니다. 표준 1203 감사 계획에 자세히 설명된 대로, 감사 업무 계획을 설정하는 것은 감사 실무자가 감사업무 범위 안에 있는 모든 요소를 이해할 수 있게 하고, 모든 식별된 위험을 포함할 수 있게 하며, 합의된 일정 이내 감사업무가 실행되는 데 필요한 기술과 지식이 가용한지 확인할 수 있게 해 줍니다.
2204.2.2	감사 업무를 수행하는 데 있어 주요 업무는 다음과 같습니다. • **계획 및 위험 평가** • **통제 식별**—감사 범위, 감사 목적 및 IT 감사 계획에서 식별된 위험의 주요 영역을 기준으로, 감사 실무자들은 감사 업무 범위 이내에 있는 통제항목을 식별해야 합니다. • **통제 평가 및 증거 수집**—감사 실무자들은 통제의 설계 효과성 및 운영 효과성에 대한 정보 및 증거를 수집하고 분석하여 감사 범위 이내에 있는 통제항목을 평가해야 합니다. • **감사업무 수행 결과의 문서화 및 발견 사항의 식별**—감사 실무자들은 수행 결과를 문서화하고, 수집된 정보 및 증거를 기록하고, 식별된 발견사항을 문서화해야 합니다. • **발견사항 확인 및 시정조치에 대한 사후 확인**—감사 실무자들은 피감사인들에게 감사결과 발견사항에 대해 확인을 받아야 합니다. 피감사인이 감사 업무가 끝나기 전에 발견사항에 대해 시정조치를 수행하는 경우, 감사 실무자들은 수행한 조치를 문서(및 결론)에 포함할 뿐만 아니라, 원래 발견 사항도 기재해야 합니다. • **결론 도출 및 보고**—감사 실무자들은 감사 목적을 달성하는 데 있어서 발견사항이 미치는 영향을 보고해야 합니다. 감사 목적에 미치는 영향을 평가하지 않고 통제에 대한 발견사항만 집중하는 것은 (감사 목적을 달성하는 데) 충분하지 않습니다.

2204.3 역할과 책임, 지식 및 기술

2204.3.1	감사 업무 실무자들은 최소한 다음 사항을 지정하여, 전체 감사 기간에 IT 감사팀원들의 역할과 책임을 정의하고 관리해야 합니다. • 방법론 및 접근방식 설계 • 감사업무 프로그램 마련 • 감사 수행 및 검토 역할 정의 • 이슈사항, 고려사항, 문제상황 발생 시 해결 • 발견사항의 문서화 및 조치 여부 확인 • 보고서 작성

2204.3.2	감사업무 상 필요에 기반하여, 감사담당 실무 관리자들은 특정 감사 업무에 필요한 역량을 고려해야 합니다. 이들은 감사 업무를 성공적으로 완료하기 위해 기술, 지식 및 경험을 두루 갖춘 감사팀을 꾸려야 합니다. 감사 실무자들은 이러한 역할과 책임을 감사업무 요건에 가장 잘 맞는 기술을 보유한 IT 감사팀원들에게 배정하도록 해야 합니다.
2204.3.3	감사 실무자들은 자신들의 지식과 기술에 부합하는 역할과 책임 및 관련된 감사업무만 수락해야 합니다. 시간과 비용 문제 때문에 감사 실무자들은 감사 업무가 시작되기 전에 필요한 지식과 기술을 모두 획득하지 못할 수 있으므로, 성공적으로 감사업무를 완료하기 위해서는 감사 실무자들은 감사 업무 중 적절한 조치를 취해질 것으로 합리적으로 예상되는 경우에 역할, 책임 및 관련된 감사업무를 수락할 수 있습니다. 다음 조치를 통해 이러한 합리적인 기대를 할 수 있습니다. • **감사 업무를 통해 배우기**—어떤 상황에서는 감사 실무자들이 감사 중 필요한 기술 및 지식을 얻을 수 있습니다. • **감독**—감사업무 관리자들은 IT 감사팀원들을 적절하게 감독할 것을 계획하여, 감독 하에서 작업을 성공적으로 수행할 수 있도록 한다. • **외부 자원**—감사업무 관리자 들은 팀이 적절한 내부 지식과 기술을 가지고 있지 않은 감사 업무 영역에 대해 외부 전문가를 고용할 수 있습니다. 감사담당 관리자들은 외부 전문가들과 긴밀하게 협업하여 이들의 지식과 기술을 전수받을 수 있도록 하여 내부 IT 감사팀원들의 발전을 도모해야 합니다.

2204.4 감독

2204.4.1	IT 감사팀원들에 의한 감사 업무 중 수행된 모든 업무는 감사 목적 및 해당 전문가 감사 표준을 충족하기 위한 감독 책임을 맡은 감사 실무자의 감독을 받아야 합니다. 필요한 감독의 정도는 검토를 수행하는 감사 실무자의 기술, 지식, 경험과 감사 업무의 복잡도에 크게 의존합니다.
2204.4.2	감독은 감사 업무의 모든 단계에 존재하는 프로세스입니다. 감독은 다음 사항을 포함합니다. • IT 감사팀원들이 감사 업무를 성공적으로 완료하기 위해 기술, 지식 및 경험을 두루 갖추도록 해야 합니다. • 적절한 감사 업무 계획 및 감사 프로그램이 마련되고 승인되도록 해야 합니다. • 감사 조서를 검토해야 합니다. • 피감사인 및 기타 관련 이해 관계자와의 감사 업무 소통이 정확하고, 분명하고, 간결하고, 객관적이고 시기 적절해야 합니다. • 변경 사항이 사전에 교정되거나 승인되지 않았으면, 감사 업무가 끝날 때 승인된 감사 업무 프로그램이 완료되고, 감사 업무 목적이 충족되는지 확인해야 합니다. • IT 감사팀원이 기술과 지식을 발전할 수 있는 기회를 제공해야 합니다.
2204.4.3	필요한 감사 절차가 모두 수행되고, 수집된 증거가 충분하고 적절하며, 결론이 감사 발견사항, 감사 목적 및 결론 또는 의견을 적절하게 지지할 수 있도록 감사조서를 검토해야 합니다. 감사 목적을 고려할 때, 감사를 수행하는 감사 실무자들을 감독하는 IT 감사팀원들이 검토를 수행해야 합니다.
2204.4.4	검토 프로세스 중, 검토자들은 질문사항이 발생할 때 그 내용을 기록해야 합니다. 감사 실무자들이 질문에 응답할 때는 질문이 제기되었고 답변이 이루어졌음을 보여주는 증거가 유지되도록 주의를 기울여야 합니다.

2204.4.5	검토 증거를 문서화하고 보유해야 합니다. 검토를 수행하는 증거를 문서화하는 방법은 다음과 같으며, 이에 제한되지는 않습니다. • 검토 후 각 감사 조서에 서명 및 날짜 기입 • 감사 조서 검토 체크리스트 완료 • 검토 주인 감사 업무 작업 서류에 대한 참조를 제공하고 검토 성격, 시기, 범위 및 결과를 자세히 기술하는 서명된 문서 준비 검토를 전산을 통해 하거나, 문서를 통해 하거나 유효합니다.
2204.4.6	감독은 감사 실무자들의 발전과 수행 평가를 감안합니다. 검토자들은 다른 IT 감사팀원들이 수행한 감사에 대한 특권적 견해를 가지며, 이는 팀원들의 감사 수행에 대한 상세하고 적절한 평가도 감안합니다. 검토자들은 감사 수행 능력을 향상시킬 수 있는 개선 점을 찾아내고, 기술과 지식을 발전시킬 수 있는 방법을 조언해야 합니다.

2204.5 증거

2204.5.1	감사 실무자들은 감사의견을 제시하거나, 감사 결론을 지지하고, 감사 목적을 달성하기 위해 충분하고 적절한 증거를 확보해야 합니다. 감사 증거가 충분하고 적합한지 여부에 대한 판단은 감사 목적의 중요성과 감사 증거 확보에 쏟은 노력에 기반해야 합니다.
2204.5.2	감사 실무자들은 판단 상, 획득된 증거가 감사 의견을 제시하거나 결론을 지지하고 감사 목적을 달성하기에 충분하고 적절한지에 대한 요건을 충족하지 않는 경우 추가 증거를 확보해야 합니다.
2204.5.3	감사 실무자들은 감사 중인 주제 사안에 따라, 증거를 수집하기에 가장 적합한 절차를 선택해야 합니다.
2204.5.4	감사 실무자들은 감사 증거의 신뢰성을 고려해야 합니다(즉, 증거 제공자의 독립성, 정보 제공자의 적격성, 증거의 객관성 또는 증거의 시기).
2204.5.5	감사 실무자들은 감사 발견사항을 지지하고 결론을 도출하기 위해 적절한 분석 및 해석을 수행해야 합니다. 수령한 증거 및 정보는 감사 실무자들이 식별하고, 마련한 기대치와 비교해야 합니다. 감사 실무자들은 다음 사항을 알고 있어야 합니다. • 예기치 않은 차이 • 예상된 차이 없음 • 잠재적 오류 • 사기 또는 불법 행위 • 법 또는 규정 비준수 • 이례적 또는 비반복 활동
2204.5.6	기대치와의 차이가 식별되면 감사 실무자들은 차이에 대한 원인을 경영진에게 질문해야 합니다. 경영진의 설명이 감사 실무자의 전문적 판단에 비추어 적절하면, 감사 실무자들은 기대치를 수정하고 증거 및 정보를 다시 분석해야 합니다.
2204.5.7	피감사인이 적절하게 설명하지 못한 상당한 차이는 감사 발견사항으로 생성되어 경영진 또는 이사회 등 기업의 지배구조 및 감사 기능 감독을 책임지는 이들에게 전달되어야 합니다. 상황에 따라, 감사 실무자들은 적절한 조치를 취할 것을 권고할 수 있습니다.

2204.6 문서화

2204.6.1	감사 실무자들은 결론을 도출하기 위한 기준을 제공하고 수행된 검토의 증거를 포함하는 충분하고 적절하고 감사업무와 관련 있는 문서를 시기적절하게 준비해야 합니다. 충분하고 적절하고 감사업무와 관련 있는 문서는 이전에는 감사 업무와 관련이 없었고 신중하며 충분한 정보를 보유한 사람이 다시 감사를 수행하여도 동일한 결론에 도달할 수 있게 합니다. 문서에는 다음 내용이 포함되어야 합니다. ● 감사 업무 목적과 감사 범위 ● 감사 업무 계획 ● 감사 업무 프로그램 ● 수행된 감사 절차 ● 수집된 증거 ● 결론 및 권고사항
2204.6.2	문서화는 다음과 같은 이유로 감사 업무를 계획, 수행 및 검토하는데 도움을 줍니다. ● 문서를 준비하고, 검토하는 것을 통해 각 감사 업무를 수행한 IT 감사팀원을 식별하고 이들의 역할을 특정할 수 있습니다. ● 문서는 요청된 증거를 기록합니다. ● 문서는 수행된 감사의 정확성, 완전성 및 유효성 검증을 지원합니다. ● 문서는 도출된 감사 결과를 보강합니다. ● 문서는 검토 프로세스를 용이하게 합니다. ● 문서는 감사 목적이 달성되었는지 여부를 기록합니다. ● 문서는 품질 향상 프로그램에 대한 기초를 제공합니다.
2204.6.3	감사 실무자들은 감사가 시작되기 전에 검토를 위한 사전적인 프로그램을 마련해야 합니다. 감사 프로그램은 감사 실무자들이 감사의 완료를 기록하고 추후 수행되어야 할 감사대상을 식별할 수 있도록 문서화되어야 합니다. 감사가 진행됨에 따라, 감사 실무자들은 감사 기간 중 수집된 정보에 기반하여 감사 프로그램의 정확성을 평가해야 합니다. 감사 실무자들이 계획된 절차가 충분하지 않다고 판별하면 그에 따라 감사 프로그램을 수정해야 합니다.
2204.6.4	수행 및 감독 활동은 감사조서에 기록되어야 합니다. 감사조서의 설계와 내용은 특정 감사 업무의 상황에 따라 달라집니다. 그러나, IT 감사 및 보증과 관련된 관리자는 다양한 유형의 감사 업무에 대해 제한된 수의 표준 템플릿 감사조서를 만들어야 합니다. 표준 감사조서는 감사 업무의 효율성을 향상시키고 감독을 용이하게 합니다. 또한, IT 감사 및 보증과 관련된 관리자는 사용될 전달 매개체와 감사조서에 대한 보관 및 보존 절차를 결정해야 합니다.
2204.6.5	감사 실무자들은 수행된 감사의 문서화가 적시에 완료되도록 해야 합니다. 감사 결론이나 의견을 도출하는데 필요한 모든 정보 및 증거는 감사 보고서 배포 날짜 전에 확보되어야 합니다. 감사 조서에는 준비되고 검토된 날짜가 기재되어야 합니다.
2204.6.6	IT 감사 및 보증과 관련된 관리자는 감사조서를 통제하고 권한 있는 사람에게 접근 권한을 제공합니다. 외부 감사인의 감사 조서에 대한 접근 요청은 경영진 및 이사회 등 기업의 지배구조를 책임지는 담당자가 승인해야 합니다. 외부 감사인이 아닌 외부 관계자에 의한 접근 요청은 경영진 및 이사회 등 기업의 지배구조및 감사 기능 감독을 맡은 책임자가 법률전문가의 자문을 받고 승인해야 합니다.

2204.7 발견사항

2204.7.1	감사 실무자들은 수집된 증거와 정보를 분석해야 합니다. 기대치와 유의미적인 차이가 발견사항으로 도출되어야 합니다. 감사 실무자들은 피감사인과 함께 발견사항을 확인하고 통제 환경의 다른 측면에 발견사항이 미치는 영향을 평가해야 합니다.
2204.7.2	감사 실무자들은 수행할 시정조치를 제안할 수 있지만, 실행해선 안 됩니다. 피감사인이 감사가 끝나기 전에 발견사항을 교정하는 시정조치를 수행하는 경우, 감사 실무자들은 수행한 시정조치를 문서에 포함해야 합니다.
2404.7.3	감사 실무자들은 식별된 발견사항으로 결론을 도출하고 그것이 감사 목적에 미치는 영향을 평가해야 합니다. 결론을 감사 시 발견사항에 기반하여 도출해야 합니다. 시정조치를 수행한 경우, 결론에 시정조치와 원래 결론에 시정조치가 미치는 영향과 그 조치를 설명하는 부록을 만들 수 있습니다.
2404.7.4	도출된 모든 결론과 감사 목적을 달성했는지 여부를 감사 보고서에 문서화해야 합니다. 보고 표준 1401 및 지침 2401에서 자세한 보고 지침을 찾을 수 있습니다.

2204.8 기타 고려사항

2204.8.1	IT 감사 및 보증 감사 실무자는 다음을 수행해야 합니다. ● 감사업무 관련 필요 사항에 대한 기술과 경험이 일치되도록 감사팀원을 배정해야 합니다. ● 필요하다면 외부 자원을 IT 감사팀에 추가하고, 이들의 작업이 적절히 감독되도록 해야 합니다. ● 감사업무 중 특정 IT 감사 팀원의 역할과 책임을 관리하여, 최소한 다음 문제를 해결해야 합니다. ■ 실행 및 검토 역할 배정 ■ 방법론과 접근 방식 설계 책임 위임 ■ 감사 또는 보증 감사 프로그램 마련 ■ 감사업무 수행 ■ 이슈사항, 고려사항, 문제상황 발생 시 해결 ■ 근본 원인 분석 ■ 팀과 조정하여 발견사항 검토, 문서화 및 정리 ■ 보고서 작성 ● 팀원에 의해 수행된 감사업무는 다른 적절한 팀원에 의해 검토를 받도록 해야 합니다. ● 감사 목적에 대한 중요성, 감사 증거 수집 시간과 노력에 부합하여 획득할 수 있는 가장 좋은 감사 증거를 사용해야 합니다. ● 전문적인 판단 상, 획득된 증거가 감사 발견사항과 결론을 지지하거나 감사 의견을 형성하기에 충분하고 적절한 수준을 충족하지 않는 경우 추가적인 증거를 확보해야 합니다. ● 사전 정의된 문서 및 승인 절차를 따라 감사 중에 수행된 감사업무를 정리하고 문서화해야 합니다.

	• 문서에 포함되어야 할 내용:
	  ■ 감사 목적과 감사 범위, 감사 프로그램, 수행된 감사 절차, 수집된 증거, 발견사항, 결론, 권고 사항
	  ■ 신중하고 충분한 정보를 가진 사람이 수행된 감사를 재 수행해도 동일한 결론에 도달할 수 있을 정도의 세부 정보
	  ■ 각 감사를 수행한 팀원의 신원과 문서 준비 및 검토 시 각 팀원들의 역할
	  ■ 문서의 준비 및 검토일
	• 감사의 중요 영역, 발생한 이슈사항과 해결책, 피감사인 주장이 상세히 기록된 관련 서면 의견서를 피감사인으로부터 획득해야 합니다.
	• 감사와 관련한 책임 인정을 명시할 수 있도록 피감사인 의견서에 피감사인의 서명과 날짜가 있도록 합니다.
	• 감사 수행 중에 수령한 모든 서면 또는 구두 의견서를 감사조서에 기록하고 보관해야 합니다.

표준 1204 및 지침 2204를 위한 COBIT® 2019 연결

COBIT 2019 관리 목표	목적
APO07 인적 자원 관리	기업 목적을 달성할 수 있도록 인적 자원 역량을 최적화합니다.
APO08 관계 관리	올바른 지식, 기술 및 행동으로 결과를 개선하고, 자신감과 상호 신뢰를 높이고 자원을 효과적으로 사용하여 비즈니스 이해관계자들과 생산적인 관계를 증진시킬 수 있습니다.
MEA04 보증 관리	잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 계획, 범위 설정, 실행 및 사후 조치하는 과정을 가이드하여 조직이 효율적이고 효과적인 보증 계획을 설계 및 개발할 수 있도록 합니다.

수행 표준 1205: 증거

내용	**1205.1** IT 감사 및 보증 감사 실무자는 적절한 결론을 도출해내기 위한 충분하고 적절한 증거를 확보해야 합니다.
	1205.2 IT 감사 및 보증 실무자는 전문가적 의구심을 적용하여, 결론을 지지하고참여 목표를 달성하기 위해 확보한 증거의 충분성을 평가해야 합니다.
	1205.3 IT 감사 및 보증 감사 실무자는 다른 작업 서류와 함께, 공식적으로 정의되고 승인된 보존 기간과 일치하는 기간 동안 증거를 보존해야 합니다.

수행 지침 2205: 증거

2205.1 소개 이 지침의 목적은 충분하고 적절한 증거를 확보하고 수령한 증거를 평가하고 적절한 감사 문서를 준비하는 데 있어서 IT 감사 및 보증 감사 실무자들을 안내하기 위한 것입니다. 지침 내용 섹션은 다음과 같은 주요 감사 및 보증 주제에 대한 정보를 제공하도록 구조화되었습니다.

2205.2 증거 유형

2205.3 증거 확보

2205.4 증거 평가

2205.5 감사 문서 준비

2205.6 기타 고려사항

2205.2 증거 유형

2205.2.1	감사를 계획하고 수행할 때, 감사 실무자들은 수집될 증거 유형, 감사 목적을 충족하기 위한 증거의 사용, 그리고 다양한 수준의 증거 신뢰성을 고려해야 합니다. 감사 실무자들이 사용을 고려해야 하는 증거 유형은 다음과 같습니다. ● 관찰된 프로세스 및 물리적 항목의 존재 ● 기록 증거 ● 의견서 ● 분석
2205.2.2	관찰된 프로세스 및 물리적 항목의 존재는 다음과 같은 활동, 자산 및 IT 기능에 대한 관찰을 포함할 수 있습니다. ● 운영 상의 네트워크 보안 모니터링 시스템 ● 원격지 저장소 위치에서 미디어 자산내역
2205.2.3	종이 또는 다른 미디어로 기록된 증거는 다음과 같을 수 있습니다. ● 서면 정책 및 절차 ● 데이터 추출 결과 ● 트랜잭션 레코드(거래 기록) ● 프로그램 목록 ● 보통의 비즈니스 과정에서 생성된 기타 문서 및 기록 ● 제삼자로부터의 외부 확인
2205.2.4	감사 중인 사람들의 서면 또는 구두 의견서는 다음 내용을 포함할 수 있습니다. ● 새 시스템 도입에 대한 내부 통제장치 및 계획의 존재 여부 및 효과성에 대한 의견서와 같은 경영진의 서면 진술 ● 프로세스 작동 방식이나 보안 인식 프로그램과 관련된 조치에 대한 관리진의 사후 조치 계획과 같은 내용에 대한 구두 의견서
2205.2.5	또한 비교, 시뮬레이션, 계산 및 추론을 통한 정보 분석 결과도 증거로 사용될 수 있습니다. 예는 다음과 같습니다. ● 기타 기업 또는 과거 기간 대비 IT 성능 벤치마킹 ● 애플리케이션, 트랜잭션 및 사용 간 오류률 비교 ● 프로세스 또는 제어 재수행

2205.3 증거 확보

2205.3.1	감사 실무자들은 합리적인 감사 결론을 추론할 수 있는 충분하고 적절한 증거를 확보해야 합니다. 이러한 증거는 다음과 같습니다. • 수행된 절차 • 수행된 절차의 결과 • 감사를 지원하기 위해 사용된 원본 문서(전자 문서 또는 서류 형태), 레코드 및 보강 정보 • 관련 법률, 규정 및 정책에 준수하여 수행된 감사에 관한 문서
2205.3.2	구두 의견 형태로 얻은 증거가 감사 의견이나 결론에 중요한 경우, 감사 실무자들은 서면으로 또는 (이메일과 같은) 전자 양식으로, 의견서의 확인을 받을 것을 고려해야 합니다. 또한 감사 실무자들은 신뢰성을 보장하기 위해 이러한 의견서를 입증할 다른 증거도 고려해야 합니다.
2205.3.3	증거를 수집할 때, 전문가들은 다음 사항을 고려해야 합니다. • 감사 위험의 감소 측면에서 증거의 충분성 대비 증거 확보에 필요한 시간, 노력 및 비용의 정도 • 감사 목적을 달성하고 감사 위험을 줄이는 데 있어서 평가되는 문제와 증거를 요구하는 감사 절차의 중요성 • 전자적 증거는 시간이 지나면 전체적으로 또는 부분적으로 검색되지 않을 수 있습니다.
2205.3.4	증거를 수집하는 데 사용된 절차는 감사 대상이 되는 정보 시스템의 특성, 감사 시기, 감사 범위 및 목적, 전문가 판단에 따라 달라집니다. 감사 증거는 수동 감사 절차나 컴퓨터 지원 감사 기술(CAAT) 또는 이 둘을 모두 사용하여 수집할 수 있습니다. 실무자들은 IT 감사 목적과 관련하여 가장 적합한 절차를 선택해야 합니다. 다음 절차를 고려해야 합니다. • **조사 및 확인**—감사주제에 익숙한 경험 있는 사람들에게서 정보를 구하는 프로세스입니다. 경험 있는 사람이 반드시 감사 대상이 되는 기업의 구성원일 필요는 없습니다. 이 절차는 공식적인 서면 조사에서 비공식적인 구두 조사에 이르기까지 다양할 수 있습니다. • **관찰**—일반적으로 수행을 책임지는 담당자들이 수행하는 절차나 프로세스를 관찰하거나 시설, 컴퓨터 하드웨어 또는 정보 시스템 설정이나 구성과 같은 물리적 항목을 관찰합니다. 이러한 종류의 증거는 관찰이 있었던 시점으로 제한됩니다. 감사 실무자들은 프로세스나 절차 수행을 관찰하는 것이 절차나 프로세스가 수행되는 방식에 영향을 줄 수 있음을 고려해야 합니다. • **점검**—내부 또는 외부 문서 및 기록을 살펴봅니다. 점검될 항목을 종이 또는 전자 양식으로 제공할 수 있습니다. 또한 점검은 물리적 자산 조사를 포함할 수 있습니다. • **분석 절차**—데이터 내 가능한 관계 또는 데이터와 기타 관련 정보 간의 관계를 살펴보고 데이터를 평가합니다. 또한 변동, 추세 및 일관되지 않은 관계에 대한 조사도 포함합니다. • **재계산/계산**—수동으로 또는 CAAT를 사용하여 문서 또는 기록의 산술적 및 수학적 정확성을 확인하는 프로세스입니다. • **재수행**—본래는 정보 시스템 또는 기업 자체에서 실행된 절차 및/또는 통제를 독립적으로 수행하는 절차입니다. • **일반적으로 통용되는 기타 방법**—사회공학에 참여, 알려지지 않은 손님(Mystery Guest) 역할 또는 윤리적 침투 테스트 실시와 같이, 충분하고 적절한 증거를 수집하는 데 있어서 감사 실무자들이 따를 수 있는 일반적으로 통용되는 기타 절차입니다.
2205.3.5	증거를 수집할 때, 감사 실무자들은 증거를 제공하는 대상의 독립성과 적격성을 고려해야 합니다. 예를 들어, 독립적인 제삼자에게서 얻은 감사 입증 증거는 감사 대상이 되는 기업에서 얻은 감사 증거보다 더 신뢰할 수 있습니다. 일반적으로 물리적 감사 증거는 개인의 의견서보다 더 신뢰할 수 있습니다.

2205.3.6	수집된 증거가 법적 절차에서 사용될 가능성이 있는 경우, 감사 실무자들은 적절한 법률 전문가와 상담하여 증거를 수집, 발표 및 공개해야 하는 방식에 영향을 줄 특수한 요건이 있는지 여부를 판별해야 합니다.
2205.3.7	감사 실무자들이 충분한 감사 증거를 확보할 수 없는 상황에는 즉, 개인 또는 경영진이 IT 감사 목적을 달성하는데 필요한 만족스럽고 적절한 증거를 제공할 것을 거부하는 경우, 감사 실무자들은 감사 조직이 세운 절차에 따라 그러한 상황을 감사업무 관련 관리진에게, 그리고 필요한 경우 감사 거버넌스 책임자에게 공개해야 합니다. 감사 범위에 대한 제약과 제한 사항과 감사 목적의 달성에 대해서도 감사 결과 의사소통을 할때 공개해야 합니다.
2205.3.8	감사 실무자들은 감사 완료 후 증거를 다음과 같이 보유해야 합니다. ● 증거가 특정 기간 동안 감사 조직의 정책, 적절한 전문가 표준, 법률, 규정을 준수하는 형식으로 이용 가능해야 합니다. ● 증거가 전체 준비 및 보관 기간 동안 무단 공개 또는 수정으로부터 보호되어야 합니다. ● 보관 기간 종료 시 적절히 폐기되어야 합니다.

2205.4 증거 평가

2205.4.1	증거는 감사 목적이내에서 발견사항 또는 결론을 지지하기 위한 적절한 기반을 제공할 때 충분하고 적합합니다. 감사 실무자의 판단에서 증거가 이러한 기준을 충족하지 않을 때, 감사업무 실무자는 추가 증거를 확보하거나 추가 절차를 수행하여 증거와 관련된 제한사항이나 불확실성을 줄여야 합니다. 예를 들어, 생산 프로세스에서 사용된 실제 프로그램을 확인해주는 기타 증거가 수집될 때까지는 프로그램 목록이 적절한 증거가 되지 못할 수 있습니다.
2205.4.2	감사 중 얻은 증거의 신뢰성을 평가할 때, 감사 실무자들은 증거의 출처, 특성(서면, 구두, 시각적 또는 전자적), 인증(디지털 또는 수동 서명, 날짜/시간 소인 존재) 및 여러 출처의 확증 증거 간의 관계와 같은 증거의 특성과 속성을 고려해야 합니다. 일반적으로, 증거의 신뢰성은 다음과 같이, 증거를 얻는 데 사용된 절차를 바탕으로 낮음에서 높음까지 순위가 매겨집니다. ● 요청 및 확인 ● 관찰 ● 검사 ● 분석 절차 ● 재계산 또는 계산 ● 재수행 각 이전 절차에서는 일반적으로 다음과 같은 증거일 때 증거 신뢰성이 더 큽니다. ● 구두 의견서에서 얻은 형식보다는 서면 형식에 있는 증거 ● 감사를 받고 있는 대상에게서 간접적으로 받은 것이 아니라, 감사 실무자가 직접 받은 증거 ● 독립적인(조직으로부터) 정보 원천으로부터 얻어낸 증거 ● 독립적인(조직으로부터) 단체가 인증한 증거 ● 독립적인(조직으로부터) 기관이 관리한 증거
2205.4.3	감사 실무자들은 정보가 존재하는 기간 또는 실증 테스트 및 (해당되는 경우) 준거성 테스트의 성격, 시기 및 범위를 결정하는 데 필요한기간을 고려해야 합니다. 예를 들어, 전자 데이터 교환(EDI), 문서 이미지 처리(DIP) 및 스프레드시트로 처리된 증거는 파일 변경 사항이 통제되지 않거나 파일이 백업되지 않는 경우 특정 기간 이후 검색되지 않을 수 있습니다. 문서 가용성은 기업 문서 보유 정책의 영향을 받았을 수도 있습니다.

2205.4.4	독립적인 제삼자 감사가 있는 경우, 감사 실무자들은 감사 주제와 관련된 통제 테스트가 수행되었는지 여부와 그 테스트 결과를 신뢰할 수 있는지 여부를 고려해야 합니다.
2205.4.5	감사 실무자들은 자격을 갖춘 독립 감사인이 테스트를 재수행해도 동일한 결과 및 결론에 도달할 수 있을 정도로 충분하고 적절한 증거를 확보해야 합니다.

2205.5 감사 문서 준비

2205.5.1	감사 수행 중, 감사 실무자들은 확보한 증거를 문서화하고 미리 정의된 기간 동안 기업 정책과 관련 전문가 표준, 법 및 규정을 준수하는 형식으로, 문서가 보존되고 사용될 수 있도록 해야 합니다.
2205.5.2	감사 수행 중 확보한 증거는 적절하게 식별되고 상호 참조되고 분류되어 증거의 전체 충분성과 적절성을 쉽게 판별할 수 있도록 해야 합니다. 감사 목적의 맥락에서 발견사항 및 결론에 대한 합리적 기준을 제공하고, 다른 IT 감사팀원 또는 독립적인(조직으로부터) 단체가 쉽게 검색할 수 있도록 하려면 이러한 단계가 필요합니다.
2205.5.3	감사 실무자들은 증거 문서를 전체 준비 및 보존 기간 동안 무단 접근 및 공개,수정으로부터 보호되어야 합니다. 보존 기간은 외부 요건의 영향을 받을 수 있습니다. 예를 들어, 미국 증권거래위원회(SEC) 요건을 따라야 하는 기업의 경우, 회계 감사자는 감사 또는 검토 결론을 도출한 날로부터 7년 간의 특정 레코드를 보유해야 합니다.[1]
2205.5.4	감사 실무자들은 설정된 보유 기간이 끝나면 증거 문서를 폐기해야 합니다.

2205.6 기타 고려사항

2205.6.1	감사 수행 시, IT 감사 및 보증 감사 실무자는 다음을 수행해야 합니다. • 적절하게 증거를 식별하고, 상호 참조하고, 분류해야 합니다. • 감사의 목표와 위험을 만족시키기 위해 필요한 증거를 수집하는 가장 비용 효과적이고 적시적인 수단을 고려해야 합니다. 그러나, 난이도 또는 비용은 필요한 절차를 제거하기 위한 적절한 기준이 될 수는 없습니다. • 관련 항목 및 위험의 중요도에 상응하는 증거를 확보해야 합니다. • 기업으로부터 획득된 정보가 감사 절차 수행을 위해 IT 감사 및 보증 감사 실무자에 의해 사용될 경우, 정보의 정확성과 완전성을 충분하게 강조해야 합니다.

표준 1205 및 지침 2205를 위한 COBIT® 2019 연결

COBIT 2019 관리 목표	목적
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

[1] 미국 증권거래위원회, "최종 규칙: 감사 및 검토와 관련된 레코드 보유", *www.sec.gov/rules/final/33-8180.htm#:~:text=Under%20the%20new%20rule%2C96,of%20the%20audit%20or%20review*

수행 표준 1206: 외부 전문가의 활용

내용	**1206.1** IT 감사 및 보증 감사 실무자는 해당될 경우 감사를 위해 외부 전문가를 활용하는 것을 고려해야 합니다.
	1206.2 IT 감사 및 보증 감사 실무자는 감사 실시 이전 외부 전문가의 전문 자격, 역량, 관련 경험, 자원, 독립성 및 품질 관리 프로세스의 적정성을 평가하고 승인해야 합니다.
	1206.3 IT 감사 및 보증 감사 실무자는 감사의 일환으로서 외부 전문가의 감사결과를 평가, 검토하고, 이 결과의 사용 및 의존 정도에 대한 결론을 문서화해야 합니다.
	1206.4 IT 감사 및 보증 감사 실무자는 피감사 부서에 속하지 않은 외부 전문가의 감사결과가 현재 감사목표를 달성하는데 적절하고 완전한지 여부를 결정해야 합니다. 또한 감사 실무자는 결론을 명확하게 문서화해야 합니다.
	1206.5 IT 감사 및 보증 감사 실무자는 외부 전문가의 감사결과가 감사 보고서에 직접 포함될지 또는 별도로 언급될지 여부를 결정해야 합니다.
	1206.6 IT 감사 및 보증 감사 실무자는 외부 전문가가 충분하고 적절한 증거를 제공하지 못하는 경우에 충분하고 적절한 증거를 얻을 수 있는 추가 테스트 절차를 적용해야 합니다.
	1206.7 IT 감사 및 보증 감사 실무자는 감사 의견 또는 결론을 제공하고 필요한 증거가 추가 테스트 절차를 통해서도 획득되지 않은 범위 제약 사항을 감사의견 또는 결론에 포함해야 합니다.

수행 지침 2206: 외부 전문가의 활용

2206.1 소개 이 지침은 외부 전문가의 활용을 고려하는 IT 감사 및 보증 감사 실무자에게 안내를 제공합니다. 지침 내용 섹션은 다음과 같은 주요 감사 및 보증 감사 주제에 대한 정보를 제공하도록 구성되었습니다.

2206.2 외부 전문가 활용시 고려사항

2206.3 외부 전문가의 적정성 평가

2206.4 외부 전문가의 감사 계획 및 검토

2206.5 외부 전문가의 감사업무 평가

2206.6 추가 테스트 절차

2206.7 감사 의견 또는 결론

2206.8 기타 고려사항

2206.2 외부 전문가 활용시 고려사항

2206.2.1	전체적으로 또는 부분적으로, 감사를 수행하는 데 필요한 역량이 없는 감사 실무자들은 필요한 기술을 가진 외부 전문가의 도움을 구할 것을 고려해야 합니다.
2206.2.2	수행될 감사 성격 상 필요한 기술 지식이 없거나, 감사 자원의 부족, 시간 제약 및 잠재적 독립성 문제와 같이, 감사 수행을 방해할 수 있는 제약 조건이 있을 경우 외부 전문가 활용을 고려해야 합니다. 또한 감사 품질을 개선할 경우에도 외부 전문가의 활용을 고려해야 합니다.

2206.2.3	감사 실무자들이 외부 전문가와 동등한 수준의 지식을 가지고 있을 것이라고 기대되지는 않습니다. 그러나, 감사 실무자들은 외부 전문가에게 감사 업무를 안내하고 그 결과를 검토할 수 있으려면 수행된 감사에 대한 충분한 지식을 가지고 있어야 합니다. 외부 전문가에게 감사업무를 의존할 때, 감사 실무자들은 전문가의 역량과 기술 수준을 검증하는 객관적인 증거를 제시해야 합니다.
2206.2.4	감사 실무자들은 특정 전문가를 선택하고, 외부 전문가의 감사업무 수행을 선택하는데 있어 객관적인 기준을 마련해야 합니다.
2206.2.5	감사 실무자들은 감사 수행 이전 외부 전문가와 계약서 또는 합의서 형태로 수행 요건을 협의하고, 그 내용을 문서화해야 합니다.
2206.2.6	레코드 또는 시스템에 대한 외부 전문가의 접근이 기업의 내부 정책에 따라 금지된 경우, 감사 실무자들은 외부 전문가의 감사업무에 대한 적절한 활용 및 의존 정도를 결정해야 합니다.
2206.2.7	필요한 외부 전문가를 확보할 수 없는 경우, 감사 실무자들은 감사 목적을 달성하는 데 있어서 그 영향을 문서화하고 그에 따른 감사 위험을 관리하기 위한 구체적인 업무를 감사 계획에 포함해야 합니다. 감사 위험을 관리할 수 없는 경우, 감사 실무자들은 그 감사를 거부해야 할 수 있습니다.
2206.2.8	IT 감사 및 보증 감사 실무자들은 시스템 및 조직 통제(SOC) 보고서에 대한 의존성을 검토할 수 있습니다.

2206.3 외부 전문가의 적정성 평가

2206.3.1	특정 감사에 외부 전문가의 활용을 포함할 경우, IT감사를 계획할 때 감사 실무자들은 외부 전문가의 전문적 자격, 역량, 관련 경험, 자원 및 품질 관리 프로세스 사용을 평가하여 외부 전문가의 적절성을 고려해야 합니다.
2206.3.2	감사 실무자들은 외부 전문가의 감사업무에 의존하기 전에 이들 전문가의 독립성과 객관성을 고려해야 합니다. 외부 전문가의 독립성 및 객관성에 대한 일반적인 지표는 외부 전문가의 선정 및 임명 프로세스, 조직의 상태, 보고 라인 및 외부 전문가의 추천이 경영진의 실무에 미치는 영향에 대한 절차입니다.

2206.4 외부 전문가의 감사 계획 및 검토

2206.4.1	감사 실무자들은 감사 헌장 또는 감사 계약서에 외부 전문가의 감사에 대한 접근 권한이 지정되어 있음을 확인해야 합니다. 법적인 또는 사생활 침해 문제가 발생하지 않는 범위에서 감사 실무자들은 외부 전문가가 작성한 모든 감사조서, 관련 문서 및 보고서에 대한 접근 권한을 가지고 있어야 합니다.
2206.4.2	감사 실무자들은 다음을 포함하여, IT 감사를 계획하면서 외부 전문가의 활동과 이들의 활동이 IT 감사 목적에 미치는 영향을 고려해야 합니다. • 외부 전문가의 감사 범위, 접근방식, 시기 및 품질 관리 프로세스 사용에 대한 이해 • 필요한 검토 수준 판별
2206.4.3	필요한 감사 증거의 성격, 시기 및 범위는 외부 전문가의 감사 중요성과 범위에 따라 달라집니다. 감사 계획 중, 감사 실무자들은 전체 IT 감사 목적을 효과적으로 달성하기 위해 충분하고 적절한 감사 증거를 제공해야 하는 검토 수준을 식별해야 합니다. 감사 실무자들은 외부 전문가의 최종 보고서, 방법론 또는 감사 프로그램과 감사 조서를 검토해야 합니다.
2206.4.4	감사 조서를 검토할 때, 감사 실무자들은 제공된 감사 증거의 적합성과 충분성을 고려하고, 외부 전문가 활용 및 의존 정도를 판별하기 위해 외부 전문가의 감사업무가 적절하게 계획되고, 감독되고, 문서화되고, 검토 되었는지를 평가해야 합니다. 이 평가는 외부 전문가의 감사결과를 다시 테스트하는 것을 포함할 수 있습니다. 관련 전문적인 표준의 준수도 평가해야 합니다. 전반적으로 감사 실무자들은 외부 전문가의 감사업무가 현재 IT 감사 목적에 대한 결론을 도출하고 결론을 문서화할 수 있도록 적절하고 완전한 지를 평가해야 합니다.

2206.4.5	감사 실무자들은 외부 전문가의 최종 보고서를 충분히 검토하여 다음 사항을 확인해야 합니다. • 감사 헌장, 운영 지침 또는 계약서에 지정된 범위가 충족됨. • 외부 전문가가 사용한 중요한 가정이 식별됨. • 보고된 발견사항 및 결론이 적절하게 증거로 뒷받침됨.

2206.5 외부 전문가 감사결과의 평가

2206.5.1	비핵심적인 활동의 처리 및 아웃소싱에 대하여 고객과 공급업체 간의 상호 의존성은 복잡한 감사 환경에 기여합니다. 감사 대상이 되는 환경의 일부분은 다른 독립적인 기능 또는 기업에 의해 통제되고 감사될 수 있습니다. 아웃소싱 기업은 아웃소싱된 사업의 통제 환경에 대하여 이러한 제삼자가 작성한 보고서를 받습니다. 경우에 따라, 이러한 사업은 감사 실무자들이 관련 문서 및 조서에 대한 접근 권한을 가지고 있지 않음에도 불구하고 IT 감사 범위에 대한 필요를 줄여줄 수 있습니다. 감사 실무자들은 이러한 경우에 대한 견해를 밝힐 때 주의해야 합니다.
2206.5.2	감사 실무자들은 외부 전문가가 수행한 감사결과의 유용성과 적합성을 평가하고 외부 전문가가 보고한 중요한 발견사항을 고려해야 합니다. 감사 실무자들은 보고서에 직접 반영하거나 별도로 언급하든, 외부 전문가의 감사결과에 의존할 범위를 결정해야 합니다. 또한 감사 실무자들은 외부 전문가의 발견사항 및 결론이 전체 IT 감사 목적에 미치는 영향을 평가해야 합니다. 또한 감사 실무자들은 전체 IT 감사 목적을 충족하는 데 필요한 추가적인 감사업무가 완료되었는지도 확인해야 합니다. 외부 전문가에 의한 모든 의견 표명은 경영진에 의해 확인되고 공식적으로 승인되어야 합니다. 이 주제에 대한 자세한 안내는 표준 1007 의견 표명에서 찾을 수 있습니다.

2206.6 추가 테스트 절차

2206.6.1	외부 전문가의 감사결과에 대한 평가를 바탕으로, 외부 전문가의 감사결과에서 충분하고 적절한 감사 증거가 제공되지 않을 경우, 감사 실무자들은 추가 테스트 절차를 적용하여 이러한 증거를 확보해야 합니다.
2206.6.2	감사 실무자들은 외부 전문가의 감사결과에 대한 보충 테스트가 필요한지 여부를 고려해야 합니다.

2206.7 감사 의견 또는 결론

2206.7.1	감사 의견이나 결론을 도출하는 것은 감사 실무자의 책임입니다. 감사 실무자들은 외부 전문가가 수행한 작업이 감사 의견이나 결론을 지원하기에 충분한지 여부를 판별해야 합니다.
2206.7.2	수행된 추가 테스트 절차에서 충분하고 적합한 감사 증거가 제공되지 않으면, 감사 실무자들은 적합한 감사 의견이나 결론을 제공하고 필요한 경우, 범위 제한사항을 포함해야 합니다.
2206.7.3	외부 전문가의 보고서가 감사 실무자의 의견을 형성하는 데 활용된 경우 외부 전문가 보고서의 채택성 및 관련성에 대한 감사 실무자의 시각과 의견이 감사 업무 보고서에 반영되어야 합니다.
2206.7.4	적절한 경우, 감사 실무자들은 경영진이 외부 전문가의 권고사항을 이행한 정도를 고려해야 합니다. 이것은 경영진이 적절한 시간 이내 외부 전문가가 식별한 문제를 교정할 것을 약속했는지 여부와 현재 교정 상태를 평가하는 것을 포함해야 합니다.

2206.8 기타 고려사항

2206.8.1	IT 감사 및 보증 감사 실무자는 다음을 수행해야 합니다. • 필요한 외부 전문가를 조달할 수 없을 경우 감사 목표 달성에 미칠 수 있는 영향을 문서화하고, 감사 계획서에 구체적인 내용을 포함시켜 위험 및 증거 요건을 관리해야 합니다. • 외부 전문가가 법적 문제로 인해 레코드 접근 권한을 부여 받지 않은 경우, 외부 전문가 감사결과의 사용 및 의존 정도를 결정하고 이에 관해 결론을 내려야 합니다. • 외부 전문가의 활용을 보고서에 문서화해야 합니다.

표준 1206 및 지침 2206을 위한 COBIT® 2019 연결

COBIT 2019 관리 목표	목적
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

수행 표준 1207: 부정 및 불법 행위

내용	**1207.1** IT 감사 및 보증 감사 실무자는 감사 중 부정 및 불법 행위의 위험을 고려해야 합니다.
	1207.2 IT 감사 및 보증 감사 실무자는 부정 또는 불법 행위를 문서화하고 관련 담당자에게 적시에 전달해야 합니다. 일부 의사소통(예: 감독당국)은 제한될 수 있습니다. 따라서, 감사 실무자가 의사소통할 때 감사 기능의 지배구조 및 감독 책임자(예: 이사회 및/또는 감사 위원회)와 논의해야 할 수 있습니다.

수행 지침 2207: 부정 및 불법 행위

2207.1 소개 이 지침은 부정 및 불법 행위에 관하여 경영진과 IT 감사 및 보증 감사 실무자 모두의 책임을 자세히 설명합니다. 지침 내용 섹션은 다음과 같은 주요 감사 및 보증 감사 주제에 대한 정보를 제공하도록 구성되었습니다.

2207.2 부정 및 불법 행위

2207.3 경영진의 책임

2207.4 감사 실무자의 책임

2207.5 감사 계획 과정에서의 부정 및 불법 행위(에 대한 고려)

2207.6 감사 절차 설계 및 검토

2207.7 부정 및 불법 행위에 대한 대응

2207.8 내부 보고

2207.9 외부 보고

2207.10 기타 고려사항

2207.2 부정 및 불법 행위

2207.2.1	부정 및 불법 행위는 재정 및 평판에 영향을 주고 직원의 생산성과 유지력에 간접적으로 영향을 주는 등 다양한 형태로 기업에 직접적으로 부정적인 영향을 미칠 수 있습니다. 기업이 부정 및 불법 행위를 빨리 식별하기 위해 인식, 예방 및 탐지 메커니즘을 적절히 구축하는 것이 중요합니다. 부정 및 불법 행위는 통제항목이 존재하지 않거나, 허술하게 설계되거나, 오작동하는 경우 더 발생하기 쉬울 수 있습니다.
2207.2.2	부정 및 불법 행위는 기업 내 모든 수준에 있는 직원이 저지를 수 있습니다. 여기엔 다음과 같은 활동을 포함하며, 이에 제한되지는 않습니다. ● 사기(불법적 이득을 얻기 위해 다른 사람을 속이는 것과 관련된 모든 행동) ● 이득을 얻거나, 부정 또는 불법 행위를 숨길 목적으로 고의적으로 사실을 왜곡 ● IT 시스템 또는 프로세스가 관련 법과 규정을 충족하는지 여부를 보증하는데 실패한 경우를 포함하여, 법 및 규정 미준수행위 ● 사생활 침해 관련 법 적용 대상인 데이터의 무단 공개 ● 사생활 침해 관련 법 및 규정을 위반하는 데이터 보유 관행 ● 은행, 공급업체, 외주업체, 서비스 제공업체 및 이해관계자와 같은 외부 기관과 체결한 기업간 합의 및 계약에 대한 비준수 행위 ● 전자 양식으로든 또는 종이 양식으로든, 레코드 또는 문서의 조작, 변조, 위조 또는 변경 ● 전자 양식으로든 또는 종이 양식으로든, 레코드 또는 문서에서 트랜잭션 효과 억제 또는 생략 ● 부적절하거나 고의적인 기밀 정보 유출 ● 실체가 없거나 거짓으로 알려진 기록 트랜잭션(전자 양식 또는 종이 양식). 예: 허위 지출, 임금대장 사기, 탈세 ● 자산 유용 및 오용 ● 소득 은폐 또는 위탁금 유용과 같은 현금이 기업의 재무 레코드에 기록되기 전 현금의 횡령 ● 의도적이든 아니든, 저작권, 상표 및 특허와 같은 지적재산권(IP)을 위반하는 행위 ● 정보 및 시스템에 대한 허가되지 않은 접근권한 부여 ● 데이터 및 시스템에 대한 무단 액세스로 인해 발생하는 재무 또는 기타 레코드의 오류
2207.2.3	특정 행위가 불법적인지 여부에 대한 판별은 일반적으로 정통한 법률 전문가의 조언에 기반하거나 법원의 최종 판결을 기다려야 할 수 있습니다. 감사 실무자들은 불법으로 의심되는 행위이든 또는 불법으로 입증된 행위이든 상관없이, 이상 행동의 영향 또는 잠재적 영향에 주된 관심을 기울여야 합니다.
2207.2.4	모든 부정행위가 다 사기 행위로 간주되어선 안 됩니다. 사기 행위의 판별은 각 사법권의 사기에 대한 법적 정의에 따라 달라집니다. 사기 부정행위는 다음과 같은 행위를 포함하되, 이에 제한되지는 않습니다. ● 사기 영속성을 은폐하기 위한 의도를 가지고 고의적으로 통제를 우회하는 행위 ● 허가되지 않은 자산 또는 서비스 사용 ● 이러한 유형의 활동을 은폐할 것을 사주하거나 돕는 행위 비 사기적 부정행위는 다음을 포함할 수 있습니다. ● 중대 과실 ● 의도치 않은 불법 행위

2207.2.5	잠재적인 불법 행위나 사기를 보고한 후 감사 실무자들이 보복 또는 협박을 경험하는 경우가 있을 수 있습니다. 관련자들을 고려하여, 최고 감사 책임자(CAE)(또는 부사장/감사 담당 이사), 최고 경영진, 이사회 등 기업의 지배구조에 대한 책임자 및 감사 기능에 대한 감독기구(예: 이사회 및/또는 감사 위원회)는 법률 전문가과 협력하여 사안을 해결해야 합니다. 이들의 노력은 위협 또는 협박과 관련된 문제를 해결할 조치를 포함해야 하고 국내법 집행 기관과의 조정을 포함할 수 있습니다.

2207.3 경영진의 책임

2207.3.1	부정 및 불법 행위의 저지, 예방 및 탐지하기 위한 통제를 제공하는 것은 경영진 및 이사회의 주된 책임입니다.
2207.3.2	일반적으로 경영진은 다음 조치를 통하여 부정 및 불법 행위가 시기적절하게 저지, 예방 또는 탐지되는 합리적 보증을 얻습니다. ● 트랜잭션 검토 및 승인, 경영진 검토 절차를 포함하여 부정 또는 불법 행위를 예방하고 탐지하기 위한 내부 통제 시스템 설계, 구현 및 유지보수. ● 직원 행동을 감독하는 정책 및 절차 ● 컴플라이언스 검증 및 모니터링 절차 ● 부정 또는 불법 행위와 관련된 사건을 보고, 기록 및 관리하기 적합한 시스템 설계, 구현 및 유지보수 ● 컴플라이언스 및 규제 요건을 감독하는 정책 및 절차
2207.3.3	경영진은 감사 실무자들에게 부정 또는 불법 행위에 대한 지식, 영향 받은 영역을 공개해야 하고, 이러한 행위 혐의가 제기되든, 의심되든, 증명되든 취해진 조치 또한 공개해야 합니다.
2207.3.4	부정 또는 불법적인 행위 혐의가 제기되거나 , 의심 또는 감지되는 경우, 경영진은 조사 및 질의 과정을 지원해야 합니다.

2207.4 감사 실무자의 책임

2207.4.1	감사 실무자들은 모든 감사 업무에 있어 책임관계를 명확히 하기 위해 감사 헌장에 부정행위를 예방, 탐지 및 보고하는 것에 대한 경영진의 책임 및 IT 감사 및 보증 경영진의 책임을 정의할 것을 고려해야 합니다. 이러한 책임이 기업 정책이나 유사한 문서에 문서화되어 있는 경우, 감사 헌장은 그러한 영향에 대한 내용을 포함해야 합니다.
2207.4.2	감사 실무자들은 통제 메커니즘이 부정 또는 불법 행위의 발생 가능성을 완전히 제거할 수 없다는 것을 이해하여야 합니다. 감사 실무자들은 부정 또는 불법 행위의 위험을 평가하고, 식별된 부정행위의 영향을 평가하고, 감사 업무의 특성에 적합한 테스트를 설계하고 수행하는 일을 책임집니다.
2207.4.3	감사 실무자들은 부정 또는 불법 행위를 예방 또는 적발하는 일은 책임지지 않습니다. 감사 업무로 부정행위가 적발될 것이라고 보증할 수는 없습니다. 감사가 적절하게 계획되고 수행되더라도, 부정행위가 적발되지 않을 수 있습니다. 예를 들어, 직원 간 또는 직원과 외부인 간에 결탁이 있거나 경영진이 부정행위에 관여된 경우 부정행위가 적발되지 않을 수 있습니다. 감사 목적은 통제항목이 적절히 준비되고, 적당하고, 효과적이며, 준수되었음을 확인하는 것입니다.
2207.4.4	부정행위 또는 불법 행위의 존재에 대한 특정 정보가 있는 감사 실무자는 이를 보고할 의무가 있습니다.
2207.4.5	감사 실무자는 잠재적 부정 또는 불법 행위에 대한 위험 수준이 높은 상황이 식별되었다면, 실제 그 행위가 전혀 발견되지 않았다 하더라도, 경영진 및 이사회 등 기업의 지배구조에 대한 책임자들에게 알려야 합니다.
2207.4.6	감사 실무자들은 부정 또는 불법 행위의 발생에 기여할 수 있는 위험 요인을 식별할 수 있으려면 검토 중인 영역에 충분히 익숙해져야 합니다.

2207.5 감사 계획 과정에서의 부정 및 불법 행위(에 대한 고려)

2207.5.1	감사 실무자들은 적절한 방법론을 사용한 후 감사 중인 영역과 관련된 부정 또는 불법 행위의 발생 위험을 평가해야 합니다. 이 평가를 준비할 때, 감사 실무자들은 다음 요인을 고려해야 합니다. • 회사 윤리, 조직 구조, 감독의 적절성, 보상 및 포상 구조, 회사 성과에 대한 압박 정도 및 기업 방향성과 같은 조직의 특성 • 기업의 역사, 과거 부정행위 발생, 부정행위와 관련된 발견사항을 완화하거나 최소화하기 위해 후속하여 취한 활동 • 관리, 운영 또는 IT 시스템의 최근 변경 사항 및 기업의 현재 전략적 방향 • 새로운 전략적 협력관계로 초래된 영향 • 보유 자산의 종류, 제공된 서비스의 유형 및 부정행위에 대한 민감성 • 설정된 통제를 피하거나 우회할 수 있는 관련 통제 및 취약성의 강도 평가 • 관련 규정 또는 법적 요건 • 내부고발자 정책, 내부자 거래 정책, 직원 및 경영진 윤리강령 등과 같은 내부 정책 • 이해 관계자 관계 및 금융 시장 • 인적 자원 역량 • 주요 시장 정보의 기밀성 및 무결성 • 이전 감사의 발견사항 • 기업이 운영되는 산업 및 경쟁적 환경 • 컨설턴트, 품질 보증 팀 또는 특정 경영진 조사를 통한 발견사항과 같이, 감사 범위 밖에서 도출된 발견사항에 대한 검토 • 일상 업무 수행을 통한 발견사항 • 프로세스 문서 및/또는 품질 관리 서비스의 존재 • 감사 중인 영역을 지원하는 정보 시스템의 기술적 정교함 및 복잡성 • 패키지 소프트웨어에 대비되는 핵심 업무를 위한 사내 개발/유지보수 애플리케이션 시스템의 존재 • 직원 불만족 영향 • 잠재적 정리 해고, 아웃소싱, 기업 분할 또는 구조 조정 • 유용하기 쉬운 자산의 존재 • 조직의 재정 및/또는 운영 성과 저조 • 윤리에 대한 경영진의 태도 • 특정 산업에 일반적이거나 유사한 기업에서 발생한 부정 및 불법 행위

2207.5.2	위험 평가의 계획 프로세스 및 수행 과정에서, 다음에 해당하는 경우 감사 실무자들은 경영진에게 질문해야 하고, 서면 의견서를 얻어야 합니다. • 기업에서 부정 및 불법 행위의 위험 수준에 대한 경영진의 이해 • 경영진이 기업 내에서 발생했거나 발생했었을 수 있는 부정 및 불법 행위에 대한 지식을 가지고 있는지, 또는 해당 행위를 지시했었는지 여부 • 부정 및 불법 행위를 예방하기 위한 내부 통제의 계획과 적용에 대한 경영진의 책임 • 부정 또는 불법 행위의 위험이 모니터링되거나 관리되는 방식 • 부정 또는 불법 행위의 혐의가 있거나, 의심되거나 또는 존재하는 경우, 이를 해당 이해관계자들에게 알리기 위해 구축된 프로세스 • 조직이 운영되는 사법권에서 적용될 수 있는 국내 및 지역법과 법무부서가 위험 위원회 및/또는 감사 위원회와 협조하는 정도

2207.6 감사 절차 설계 및 검토

2207.6.1	감사 실무자들에게 불법 또는 부정행위를 적발하거나 예방해야 하는 명시적 책임은 없지만, 감사 실무자들은 식별된 부정 및 불법 행위를 고려하는 감사 절차를 설계해야 합니다.
2207.6.2	감사 실무자들은 위험 평가의 결과를 사용하여 다음 사항이 식별되었다는 합리적 확신에 필요한 충분한 감사 증거를 확보하기 위해 테스트의 성격, 시기 및 범위를 정해야 합니다. • 감사 중인 영역 또는 기업 전체에 상당한 영향을 미칠 수 있는 부정행위 • 중요한 부정행위를 예방하거나 탐지하지 못한 통제 약점 • 비즈니스 데이터를 기록, 처리, 요약 및 보고하는 발행자의 능력에 잠재적으로 영향을 줄 수 있는 내부 통제 설계 또는 운영에 있는 모든 중요한 결점
2207.6.3	감사 실무자들은 부정 또는 불법 행위가 발생했을 수 있는 조짐을 발견하기 위해 감사 절차의 결과를 검토해야 합니다. 컴퓨터 지원 감사 기술(CAAT)을 사용하면 부정 또는 불법 행위를 효과적이고 효율적으로 적발하는 데 크게 도움이 될 수 있습니다.
2207.6.4	감사 절차의 결과를 평가할 때, 모든 식별된 위험이 포함되었다는 합리적 보증을 제공하기 위해 실제 수행된 감사절차를 통해 식별된 위험 요인을 검토해야 합니다.

2207.7 부정 및 불법 행위에 대한 대응

2207.7.1	감사 중, 부정 또는 불법 행위의 존재에 대한 징후는 감사 실무자의 주의를 끌 수 있습니다. 감사 실무자들은 부정 또는 불법 행위가 감사 주제, 감사 목적, 감사 보고서 및 기업에 미치는 잠재적 영향을 고려해야 합니다.
2207.7.2	감사 실무자들은 전문가적 의구심을 지닌 태도를 보여야 합니다. 부정 또는 불법 행위를 저지르는 사람에 대한 지표(때때로 "사기" 또는 "사기 징후"라고 함)는 다음과 같습니다. ● 경영진의 통제장치 우회 ● 불규칙하거나 잘못 설명된 경영진의 행동 ● 설정된 목표에 비해, 일관된 초과 성과 ● 요청된 정보 또는 증거 회신에 대한 문제 또는 지연 ● 정상적인 승인 주기를 따르지 않는 트랜잭션 ● 특정 고객의 활동 증가 ● 고객의 불만 증가 ● 일부 애플리케이션 또는 사용자에 대한 접근 통제 이상 감사 실무자들은 이러한 지표를 발견할 경우 각별히 주의를 기울여야 합니다.
2207.7.3	감사 실무자들은 가능한 부정 또는 불법 행위에 대한 정보를 알게 되면, 적절한 법률 당국으로 부터 안내를 받은 후 다음 단계를 수행할 것을 고려해야 합니다. ● 행위의 성격을 이해함 ● 행위가 발생한 상황을 이해함 ● 행위에 대한 증거를 수집함(예: 서류, 시스템 레코드, 컴퓨터 파일, 보안 로그, 고객 또는 공급업체 정보) ● 행위를 저지르는 데 관여한 모든 사람을 식별함 ● 행위의 영향을 평가하는 데 충분한 뒷받침 정보를 확보함 ● 행위의 영향과 추가 행위가 있는지 여부를 판별하기 위한 제한된 추가 절차를 수행함 ● 모든 증거 및 수행된 감사 결과를 기록하고 보존함
2207.7.4	가능한 부정 또는 불법 행위와 관련된 적절한 조치를 취한 후, 감사 실무자들은 감사업무 관련 경영진과 상의하여 기업 경영진에 "이벤트" 보고, 내부 사기 조사자에게 추가 조치 전달 및/또는 법 집행 또는 규제기관에 보고와 같은 다음 조치를 정해야 합니다.
2207.7.5	부정에 경영진 구성원이 관여될 때, 감사 실무자들은 경영진이 작성한 의견서의 신뢰성을 재고해야 합니다. 감사 실무자들은 적절한 수준의 경영진, 일반적으로 부정 또는 불법 행위와 관련된 인원보다 높은 수준의 경영진과 함께 업무를 수행해야 합니다.

2207.8 내부 보고

2207.8.1	감사 실무자들은 부정 및 불법 행위의 탐지를 기업의 적절한 사람에게 서면으로 또는 구두로, 시기적절하게 전달해야 합니다. 알림은 부정 및 불법 행위가 발생했다고 의심되는 수준보다 높은 수준의 경영진에게 전달되어야 합니다. 뿐만 아니라, 부정 및 불법 행위는 이사회, 이사, 감사 위원회 또는 그와 동등한 기구와 같은 기업 지배구조 책임자에게 보고되어야 합니다. 재무적 효과와 통제 약점의 징후 모두에서 명백하게 경미한 사안은 더 높은 수준으로 보고하지 않아도 됩니다. 감사 실무자가 경영진의 모든 수준이 관련되었다고 의심하면, 발견사항은 지역 해당 법과 규정에 따라, 이사회, 이사, 감사 위원회 또는 그와 동등한 기구와 같은 기업 지배구조 책임자에게 직접 기밀로 보고되어야 합니다. 지역 법과 규정에 따라 규정된 법률 당국이 아닌 다른 측에 보고 행위는 금지될 수 있습니다.
2207.8.2	이들은 관련된 것으로 보이는 개인 보다 한 단계 이상 높은 적절한 수준의 경영진과 함께 발견사항과 수행될 추가적인 절차의 성격, 시기 및 범위를 논의해야 합니다. 이들은 관련된 것으로 보이는 개인 수준보다 한 수준 이상 높은 적절한 수준의 관리진과 함께 결과와 수행될 추가 절차의 성격, 시기 및 범위를 논의해야 합니다. 이러한 상황에서는 감사 실무자들이 독립성을 유지하는 것이 특히 중요합니다.
2207.8.3	감사 실무자들은 부정 또는 불법 행위에 대한 보고서의 내부 배포에 포함할 개인을 신중하게 고려해야 합니다. 부정 또는 불법 행위의 발생 및 영향에 대한 식별은 민감한 문제이며, 보고 배포는 다음과 같은 위험을 수반합니다. ● 통제 약점에 대한 세부사항의 게시에 따른 추가적인 약점 이용 ● 기업 외부로 (허가 또는 허가되지 않은) 공개 시 고객, 공급업체 및 투자자 유실 ● 경영진과 기업 미래에 대한 신뢰 하락으로 부정 또는 불법 행위 및 기업의 미래와 관련되지 않은 사람들을 포함하여, 주요 실무자 및 경영진 유실
2207.8.4	감사 실무자들은 보고서의 배포를 통제하는 방법으로 다른 감사 문제와 별도로 부정 또는 불법 행위를 보고할 것을 고려해야 합니다.
2207.8.5	감사 실무자들은 부정 또는 불법 행위에 연루되었음을 시사하거나 연루될 수 있는 사람이 증거를 파기하거나 숨길 가능성을 줄이기 위해 이들에게 알리지 않도록 해야 합니다.
2207.8.6	감사 헌장은 부정 또는 불법 행위 신고와 관련하여 감사 실무자의 책임을 정의해야 합니다.

2207.9 외부 보고

2207.9.1	사기, 부정 또는 불법 행위에 대한 외부 보고가 법적 또는 규제 의무일 수 있습니다. 이 의무는 기업 경영진, 부정행위 탐지에 관련된 개인 또는 둘 다에 적용될 수 있습니다. 감사자의 법적 보고 요건은 지역 사법권을 따르며 내부 정책 및/또는 계약상 합의를 대체합니다. 외부 보고가 필요할 수 있는 추가 상황은 다음과 같습니다. ● 법적 또는 감독의 기준 준수 ● 법원 명령 ● 정부의 재정 지원을 받는 단체를 감사하기 위한 요건에 따른, 자금 조달 기관 또는 정부 기관의 관여 ● 외부 감사자 요청
2207.9.2	외부 보고가 필요한 경우, 보고된 정보의 양식과 내용은 적절한 수준의 IT 감사 및 보증 경영진에 의해 승인되고 감사 업무의 구체적인 상황이나 적용 규정에 의해 금지된 경우가 아니면, 외부로 유출되기 전에 피감부서 경영진과 함께 검토되어야 합니다. 피감부서 경영진의 합의를 얻지 못하게 할 수 있는 특정 상황의 예는 다음과 같습니다. ● 부정 또는 불법 행위에서 피감부서 경영진의 적극적인 관여 ● 부정 또는 불법 행위에서 피감부서 경영진의 수동적인 묵인
2207.9.3	피감부서 경영진이 보고서의 외부 유출에 동의하지 않으면, 그리고 외부 보고가 법적 또는 규정 의무이면, 실무자들은 감사 위원회 및 법률 전문가에게 기업 외부로의 발견사항 보고의 타당함과 위험에 대해 자문할 것을 고려해야 합니다. 감사 실무자가 변호사의 비밀유지권에 의해 보호되는 상황에서도, 감사 실무자들은 실제로 변호사의 비밀유지권으로 보호되고 있음을 확인하기 위해 외부 공개를 하기 전에 외부의 법률 자문 및 상담을 구해야 합니다.
2207.9.4	IT 감사 및 보증 관련 경영진이 승인했을 때, 감사 실무자들은 적시에 적절한 감독당국에 부정 또는 불법 행위를 보고해야 합니다. 기업이 알려진 부정 또는 불법 행위를 공개하지 못하거나 감사 실무자들에게 이러한 발견사항을 숨길 것을 요구하는 경우, 감사 실무자들은 법률 자문 및 상담을 받아야 합니다.
2207.9.5	감사 실무자들이 부정 또는 불법 행위를 탐지할 경우, 그들은 시기적절하게 외부 감사자에게 알려야 합니다.
2207.9.6	감사 실무자는 경영진이 사기 활동을 외부 조직에 보고해야 함을 알게 될 경우, 공식적으로 경영진에게 그 책임을 조언해야 합니다.

2207.10 기타 고려사항

2207.10.1	IT 감사 및 보증 감사 실무자는 다음을 수행해야 합니다. ● 감사를 계획하고 수행하면서 다음을 통해 감사 위험을 허용 가능한 수준으로 낮추어야 합니다. ■ 부정 및 불법 행위의 위험을 평가해도 부정 및 불법 활동에 의한 중요한 오류, 통제 결함 또는 문서상의 오류가 존재할 수 있다는 점을 인식합니다. ■ 감사 주제 사안, 감사 범위 및 감사 목적과 관련되고 부정 및 불법 행위를 예방하거나 탐지하기 위한 내부 통제장치를 포함하여, 기업 및 기업의 환경을 이해합니다. ■ 경영진 혹은 기업 내 구성원들이 실제로 발생되었거나 의심이 가는 부정 및 불법 행위에 대해 알고 있는지를 판단하기 위해 충분하고 적절한 증거를 수집합니다. ● 부정 및 불법 행위로 인한 중요한 오류, 통제 결함, 문서상의 오류 위험을 나타낼 수 있는 이례적이거나 예상치 않은 연관관계를 고려합니다. ● 내부 통제의 적합성과 부정 및 불법 행위 예방 또는 적발을 의도한 통제를 경영진이 우회할 수 있는 위험성을 테스트하기 위한 절차를 설계 및 수행합니다. ● 식별된 오류, 통제 결함 또는 문서상의 오류가 부정 또는 불법 행위를 나타낼 수 있는지 여부를 평가합니다. 만약 그런 암시가 있을 경우, 관련된 감사의 다른 부분, 특히 경영진의 진술과 관련해 어떤 의미가 내포되어 있는지 고려해야 합니다. ● 부정 및 불법 행위를 방지하고 탐지하는 내부 통제의 설계 및 구현에 대한 경영진의 책임을 확인하기 위해 감사에 따라 적어도 1년에 한 번 이상, 경영진에게서 서면 의견서를 얻으십시오. ● 부정 또는 불법 행위의 결과로 존재할 수 있는 오류, 통제 결함 또는 문서상의 오류를 나타내는 위험 평가의 관련 결과를 공개합니다. ● 내부 통제에 중요한 역할을 맡고 있는 경영진 및 직원과 관련하여 기업에 영향을 주는 부정 및 불법 행위에 대한 경영진의 지식을 공개합니다. ● 직원, 전 직원, 감독당국, 그 밖의 관련자에 의해 전달된 대로 기업에 영향을 주는 부정 및 불법 행위가 제기되거나 의심되는 경우에 대한 경영진의 지식을 공개합니다. ● 적시에 다음 내용을 수행합니다. ■ 중요한 부정 또는 불법 행위가 존재할 수 있다고 파악하거나 입수한 정보를 적합한 수준의 경영진에게 전달합니다. ■ 내부 통제에 중요한 역할을 맡고 있는 경영진 또는 직원과 관련된 일체의 중요한 부정 및 불법 행위를 이사회 등 기업의 지배구조 책임자에게 전달합니다. ■ 감사범위에 속하지 않더라도, 감사 중에 파악된 부정 및 불법 행위 예방 및 방지하기 위해 설계되고 적용된 내부 통제의 중요 취약성을 이사회 등 기업의 지배구조 책임자에게 전달합니다. ■ 감사 환경에 적용되는 합법적이며 전문적인 보고 요건을 고려합니다. ■ 중요한 오류, 통제 결함, 문서상의 오류, 또는 불법 행위가 감사의 효과성에 지속적으로 영향을 미칠 경우, 감사결과에서 제외할 것을 고려합니다. ■ 이사회 등 기업의 지배구조, 감독당국, 그 밖의 구성원들에 대한 책임을 지는 이들과 경영진에게 보고된 중요한 부정 및 불법 행위에 대한 모든 전달 사항, 계획, 결과, 평가 및 결론을 문서화합니다.

표준 1207 및 지침 2207을 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM03 위험 최적화에 대한 보장	I&T 관련 기업 위험이 기업의 위험 수용범위 및 위험감수도를 초과하지 않고, 기업 가치에 대한 I&T 위험의 영향이 식별되고 관리되고, 규정 준수 실패 가능성이 최소화되도록 합니다.
APO12 위험 관리	I&T 관련 기업 위험 관리를 전반적인 전사 위험 관리(ERM)와 통합하고 I&T 관련 기업 위험의 비용과 이익을 균형 조절합니다.
MEA03 외부 요건 준수 관리	기업에 적용되는 모든 외부 요건을 준수하도록 합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

보고 표준

보고 표준 1401: 보고

내용	**1401.1** IT 감사 및 보증 실무자는 각 업무의 결과를 전달하기 위한 보고서를 제공해야 합니다.
	1401.2 IT 감사 및 보증 실무자는 감사 보고서의 결과물이 충분하고 적합한 증거에 의해 뒷받침되도록 해야 합니다.

보고 지침 2401: 보고

2401.1 소개 이 지침은 감사 업무 보고서에 포함해야 하는 모든 측면을 자세히 설명하고 IT 감사 및 보증 실무자들에게 감사 업무 보고서의 초안을 작성하고 마무리할 때 고려해야 할 사항을 제공합니다. 지침 내용 섹션은 다음과 같은 주요 감사 및 보증 감사 주제에 대한 정보를 제공하도록 구성되었습니다.

2401.2 감사 업무 보고서의 필수 내용

2401.3 후속 이벤트

2401.4 추가 통신

2401.5 기타 고려사항

2401.2 감사 업무 보고서의 필수 내용

2401.2.1	감사 보고서는 감사 업무가 ISACA의 IT 감사 및 보증 표준 혹은 다른 적용 가능한 전문가 표준에 따라 시행되었다는 진술을 포함해야 하고, 만약 이러한 표준을 비준수하는 경우는 보고서에 명확히 언급되어야 합니다. 감사 업무의 범위도 감사 보고서에 포함되어야 합니다. 범위는 감사 주제나 활동에 대한 식별 또는 설명, 검토 중인 기간 및 감사가 수행된 기간, 수행된 작업의 성격 및 범위, 범위의 자격 요건 또는 제한사항을 포함합니다.
2401.2.2	감사 보고서는 수행된 작업에 대한 요약을 포함해야 하고, 이는 보고서의 대상 사용자가 제공된 보증의 성격을 더 잘 이해하는 데 도움을 줄 것입니다.
2401.2.3	감사 보고서는 감사인의 의견을 담은 섹션을 포함해야 합니다. 감사 보고서를 작성할 때, 감사 실무자들은 주제 사안 정보를 지지하거나 반박하는 것처럼 보이는지 여부와 관계없이, 모든 관련 증거를 고려해야 합니다. 의견은 식별된 기준에 기반한 통제 절차의 결과로 뒷받침되어야 합니다. 감사 실무자들은 감사 업무 보고서의 결론을 뒷받침하기에 충분하고 적절한 증거가 확보되었는지 여부에 대해 결론을 내려야 합니다. 보고서는 모든 실질적 측면에서, 활동 영역과 관련된 통제 절차의 설계 및/또는 운영이 효과적이었는지 여부에 대한 의견을 표명해야 합니다.
2401.2.4	감사 보고서는 통제 절차의 효과성에 대하여 경영진경영진의 기술서 출처를 식별하는 진술을 포함해야 합니다. 또한, 활동 영역에 대한 통제 절차를 포함한 효과적인 내부 통제 구조를 유지하는 것도 경영진의 책임임을 유의해야 합니다.
2401.2.5	감사 보고서는 감사 목표의 식별을 포함해야 합니다.

2401.2.6	감사 보고서는 기준에 대한 설명 또는 기준의 출처 공개를 포함해야 합니다. 뿐만 아니라, 감사 실무자들은 다음 사항을 공개할 것을 고려해야 합니다. • 기준 적용에 관한 중요한 해석 • 기준이 다양한 측정 방법 중에서 선택을 허용할 때 사용된 측정 방법 • 사용된 표준 측정 방법의 변경 사항
2401.2.7	감사 보고서는 대상 수신자와 공유에 대한 제한사항을 포함해야 합니다.
2401.2.8	감사 보고서는 보고서 책임자 또는 단체의 서명과 위치를 포함해야 합니다.
2401.2.9	감사 보고서는 감사 업무 보고서의 발행 날짜를 포함해야 합니다. 대부분의 경우, 보고서의 날짜가 발행 날짜입니다. 수행된 작업의 요약에 날짜가 명기되지 않았더라도, 보고서에는 감사 작업이 수행된 날짜를 언급하는 것이 좋습니다.
2401.2.10	감사 보고서는 배포(즉, 대상 수신자 및 공유에 대한 제한사항)가 감사 헌장 또는 계약서에 따름을 언급해야 합니다. 일부 지역에서는 IT 감사 및 보증 실무자가 자격증명(예: ISACA 또는 기타 전문가 조직의 인증 번호 및/또는 회원 번호)을 공개해야 할 수 있습니다.
2401.2.11	감사 보고서는 관측 내용, 결과, 결론 및 교정 비용(판단 가능한 경우)을 포함한 권장사항을 포함해야 합니다. 결과, 결론 및 시정조치를 위한 권장사항은 경영진의 응답을 포함해야 합니다. 각 경영진 응답에 대해, 감사 실무자들은 보고된 권장사항을 이행하기 위해 제안된 조치 및 계획된 조치 일자에 대한 정보를 확보하여야 합니다. 감사 실무자와 피감인이 특정 권장사항 또는 감사 의견에 대해 동의하지 않으면 업무 보고에 상호 입장과 의견 차이의 이유를 명시할 수 있습니다. 피감인의 서면 의견은 감사 보고서의 부록, 보고서 본문 또는 자기소개서에 포함될 수 있습니다. 경영진 또는 IT 감사 및 보증 기능의 거버넌스 책임자가 이 기능이 지원하는 관점을 결정해야 합니다.

2401.3 후속 이벤트

2401.3.1	때때로 감사 주제나 활동에 상당한 영향을 미치는 이벤트가 테스트 후속으로, 감사 보고서 발행일 전에 발생합니다. 후속 이벤트라고 칭하는 이러한 상황은 어떤 주장이나 결론을 변경시킬 수 있으므로 공개해야 할 수 있습니다. 감사 업무 수행 시, 감사 실무자들은 알게 되는 후속 이벤트에 대한 정보를 고려해야 합니다. 그러나, 감사 실무자들은 후속 이벤트를 탐지할 책임을 지지 않습니다.
2401.3.2	감사 실무자들은 경영진으로부터 후속 이벤트가 발생하지 않았다는 서면 기술서를 확보해야 합니다.

2401.4 추가 통신

2401.4.1	감사 실무자들은 마무리 및 발표 전에 보고서 초안 내용을 주제 분야의 경영진과 논의하고, 최종 보고서에 결과물, 결론, 권장사항에 대한 경영진의 응답을 포함해야만 합니다.
2401.4.2	감사 실무자들은 통제 환경에서의 중대한 결함 및 약점을 거버넌스 책임자와 책임 있는 기관(해당되는 경우)에 알려야 합니다. 또한 보고서에도 결함 및 약점이 전달되었음을 명시적으로 공개해야 합니다.
2401.4.3	감사 실무자들은 중요한 정도는 아니나 사소하다고 볼 수 없는 내부 통제 결함을 경영진에게 전달해야 합니다. 이러한 경우, 감사 실무자들은 이러한 내부 통제 결함이 경영진에 전달되었음을 거버넌스 책임자나 책임 있는 기관에 알려야 합니다.

2401.4.4	감사 실무자들은 경영진으로부터 최소한 다음 표명을 인정하는 서면 기술서를 얻어야 합니다. ● 경영진은 검토 중인 운영 활동 및 정보 시스템에 대한 내부 회계 및 관리 통제 시스템을 포함하여, 적절하고 효과적인 내부 통제장치 및 검토 중인 주제 영역을 통제하는 모든 법과 규칙 및 규정을 식별하는 활동을 수립하고 유지보수하고, 이러한 법과 규정의 준수를 보장할 것을 책임집니다. ● 업무 팀에 다음을 포함하여(이에 제한되지 않음) 업무 목표와 관련된 모든 요청된 정보가 제공되었습니다. ■ 레코드, 관련 데이터, 전자 파일 및 보고서 ■ 정책 및 절차 ■ 관련 직원 ■ 관련 내부 및 외부 IT 감사, 검토 및 평가 결과 ■ 경영진은 후속 이벤트를 보고할 책임이 있습니다. ■ 경영진은 경영진과 내부 통제 책임을 지고 있는 직원들이 공개하지 않은 내용을 포함하여, 검토 중인 주제 영역과 관련된 사기 또는 의심 사기, 부정 및 불법 행위를 전혀 알지 못합니다. ■ 경영진은 드러나지 않은 직원, 고객, 계약업체 등의 전달에서 수신된 검토 중인 영역에 영향을 주는 사기 주장이나 의심 사기, 부정 및 불법 행위를 전혀 알지 못합니다. ■ 경영진은 탐지된 사기, 부정 및 불법 행위를 예방하고 발견하기 위한 프로그램 및 통제장치의 계획과 수행에 대한 책임을 인식합니다.

2401.5 기타 고려사항

2401.5.1	IT 감사 및 보증 실무자는 다음을 수행해야 합니다. ● 피감인으로부터 업무의 중요 분야, 발생한 문제와 해결책, 피감인의 주장이 상세히 기록된 관련 서면 기술서를 획득해야 합니다. ● 활동과 관련한 피감인의 책임 인정을 명시할 수 있도록 피감인 기술서에 피감인의 서명과 날짜가 있도록 합니다. ● 책임 있는 피감 경영진으로부터 서면 답변을 확보할 수 없으면 구두 답변을 얻어서 업무 서류에 문서화합니다. ● 활동 수행 과정 중에 받은 모든 서면 또는 구두 기술서를 업무 문서로 작성하고 보관합니다. 증명 활동 시, 오해 가능성을 줄일 수 있도록 피감인의 서면 기술서를 확보해야 합니다. ● 중요 취약성과 이것이 활동 목표 달성에 미치는 영향을 보고서에서 설명합니다. ● 마무리 및 발표 전에 보고서 초안 내용을 주제 분야의 경영진과 논의하고, 해당될 경우 최종 보고서에 결과물, 결론, 권장사항에 대한 경영진의 응답을 포함시킵니다. ● 상당한 결함 및 약점을 경영진과 논의한 후, 거버넌스 책임자와 책임 있는 기관(해당되는 경우)에 알립니다. 보고서에 상당한 결함 및 약점이 전달되었음을 공개합니다. ● 별도의 보고서들은 최종 보고서에 주석으로 표시합니다. ● 중요한 정도는 아니나 사소하다고 볼 수 없는 내부 통제 결함을 피감사 경영진에게 전달합니다. 이러한 경우, 감사 기능의 거버넌스 책임자 또는 책임 있는 기관에 해당 내부 통제 결함이 피감 경영진에게 전달되었음을 통보합니다. ● 업무 시행 시 적용된 표준을 식별합니다. 표준 비준수 상황이 발생되면 전달합니다.

표준 1401 및 지침 2401을 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM05 이해관계자 참여 보장	이해관계자가 I&T 전략 및 로드맵을 지지하도록 하고, 효과적이고 시의적절하게 전달되도록 하고, 성과를 높이도록 보고 기준이 설정되도록 합니다. 개선 영역을 식별하고, I&T 관련 목표와 전략이 기업의 전략과 일치하는지 확인합니다.
MEA01 수행 및 적합성 모니터링 관리	수행과 적합성의 투명성을 제공하고 목표 달성을 추진합니다.
MEA02 내부 통제 시스템 관리	내부 통제 시스템의 적절성에 대한 주요 이해관계자들의 투명성을 확보하여 운영에 대한 신뢰, 기업 목표 달성에 대한 확신, 그리고 잔여 위험에 대한 적절한 이해를 제공합니다.
MEA03 외부 요건 준수 관리	기업에 적용되는 모든 외부 요건을 준수하도록 합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드 맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

보고 표준 1402: 사후 활동

내용	**1402.1** IT 감사 및 보증 실무자는 감사 기능의 거버넌스 및 감독(예: 이사회 및/또는 감사 위원회) 책임자에게 결과 및 권장사항에 대한 경영진의 진행상황을 정기적으로 보고해야 합니다. 보고는 경영진이 보고된 감사 결과와 권장사항을 다루기 위해 적시에 적절한 조치를 계획하고 취했는지 여부에 대한 결론을 포함해야 합니다.
	1402.2 감사 결과 이행에 대한 전체 진행 상황은 감사 위원회가 설립되어 있다면 감사 위원회에 정기적으로 보고해야 합니다.
	1402.3 감사 결과에 나타난 위험이 수용되었고 기업의 위험 수용범위보다 크다고 판단될 경우, 이 위험의 수용 여부는 고위 경영진과 논의해야 합니다. 위험(특히 위험 해결 실패)의 수용은 감사 위원회(존재하는 경우) 및/또는 이사회의 주목을 받아야 합니다.

보고 지침 2402: 사후 활동

2402.1 소개 이 지침의 목적은 경영진이 보고된 권장사항 및 감사 결과에 적절한 조치를 적시에 취했는지 여부를 모니터링하는 데 안내하는 것입니다. 지침 내용 섹션은 다음과 같은 주요 감사 및 보증 감사 주제에 대한 정보를 제공하도록 구성되었습니다.

2402.2 사후 프로세스

2402.3 경영진의 제안 조치

2402.4 시정조치를 취하지 않을 경우 위험 가정

2402.5 사후 절차

2402.6 사후 활동 시기 및 일정

2402.7 사후 활동 성격 및 범위

2402.8 사후 활동 연기

2402.9 사후 대응 양식

2402.10 외부 감사 권장사항에 대한 감사 실무자의 사후 활동

2402.11 사후 활동 보고

2402.2 사후 프로세스

2402.2.1	사후 활동은 감사 실무자들이 외부 감사자 및 그 외 사람들이 작성한 보고 내용을 포함하여, 보고된 결과 및 권장사항에 대해 경영진이 취한 조치의 적절성, 효과성과 적시성을 판별하는 프로세스입니다.
2402.2.2	사후 프로세스는 감사 실무자가 실시한 각 검토에서 검토로 합의된 결과를 경영상 과제에 따라 구현할 경우 기업에 최적의 이점이 제공되거나, 임원진이 제안된 결과 및/또는 권장사항이 지연되거나 구현되지 않을 위험을 인식하고 인정한다는 합리적 확신을 제공하는 데 도움을 주도록 설정되어야 합니다.

2402.3 경영진의 제안 조치

2402.3.1	피감인과의 논의의 일환으로, 감사 실무자들은 감사 업무의 결과와 필요에 따라 운영 개선을 위한 조치계획에 대한 합의를 얻어야 합니다.
2402.3.2	감사 실무자들은 경영진과 보고된 권장사항 및 감사 의견을 구현하거나 해결하기 위해 제안된 조치를 논의해야 합니다. 제안된 조치를 감사 실무자들에게 제공해야 하고 약속된 구현 및/또는 조치 날짜를 포함한 최종 보고서에 경영진 대응으로 보고해야 합니다.
2402.3.3	감사 실무자와 피감인이 제안된 조치에 합의하게 되면 감사 실무자는 사후 활동에 대한 절차를 시작해야 합니다.

2402.4 시정조치를 취하지 않을 경우 위험 가정

2402.4.1	경영진은 시정조치의 비용, 복잡성 또는 그 밖의 고려사항 때문에 보고된 조건을 개선하지 않을 경우 발생할 위험을 감수하기로 결정할 수 있습니다. 이사진 또는 거버넌스 책임자에게 경영진이 보고된 상황을 개선하지 않고 위험을 수용할 경우 권장사항을 알려야 합니다. 위험 수용은 문서화되고 공식적으로 경영진에 의해 승인되고 거버넌스 책임자에게 전달해야 합니다.
2402.4.2	감사 실무자들이 피감인이 기업에 부적합한 잔여 위험 수준을 받아들였다고 믿으면, IT 감사 및 보증 관리자 및 경영진과 그 문제에 대해 논의해야 합니다. 감사 실무자가 잔여 위험에 대한 결정에 계속 동의하지 않으면, 이들은 경영진과 함께, 그 문제를 해결하기 위해 이사회 또는 거버넌스 책임자에게 보고해야 합니다.

2402.5 사후 절차

2402.5.1	다음을 포함하여, 사후 활동을 위한 절차를 설정해야 합니다. ● 경영진이 동의한 권장사항에 대응해야 하는 시간 기록 ● 경영진의 대응 평가 ● 해당되는 경우, 대응의 유효성 검증 ● 해당되는 경우, 사후 작업 ● 미해결 및 불만족스러운 대응 및/또는 조치를 적절한 수준의 경영진 및 거버넌스 책임자에게 에스컬레이션 하는 절차 ● 시정 조치가 지연되거나 실행을 제안하지 않는 경우, 경영진의 관련 위험에 대한 가정을 획득하는 프로세스
2402.5.2	자동 추적 시스템 또는 데이터베이스가 사후 활동 수행을 지원 할 수 있습니다.
2402.5.3	적절한 사후 절차를 정할 때 고려해야 하는 요인은 다음과 같습니다. ● 문제가 되는 IT 환경 또는 IT 애플리케이션에 대한 발견 사항 및 권장사항의 중요성과 영향도 ● 발견 사항 및 권장사항의 중요성과 영향도에 영향을 줄 수 있는 IT 환경의 변경 사항 ● 보고된 상황에 대한 시정 조치의 복잡성 ● 보고된 상황을 시정하기 위해 필요한 시간, 비용 및 노력 ● 보고된 상황의 시정 조치가 실패할 경우 영향
2402.5.4	사후 조치, 보고 및 에스컬레이션에 대한 책임은 감사 헌장에 정의되어야 합니다.

2402.6 사후 활동 시기 및 일정

2402.6.1	사후 활동의 시기에 대한 결정은 보고된 발견 사항의 중요성과 시정조치를 취하지 않을 경우 기업 전략 및 목표에 미치는 영향을 고려해야 합니다. 최초의 보고와 관련하여 사후 활동의 시기는 기업에 대한 관련 위험 및 비용의 특성 또는 정도 등 여러 고려 사항에 따라 전문적으로 판단할 사항입니다.
2402.6.2	사후 활동은 IT 감사 프로세스의 핵심 부분이므로, 각 검토를 수행하는 데 필요한 다른 단계와 함께 사후 활동 일정을 수립해야 합니다. 특정 사후 활동과 이러한 활동의 수행 시기는 난이도, 관련 위험 및 노출, 검토 결과, 시정 조치를 이행하는 데 필요한 시간 및 기타 요인들의 영향을 받을 수 있으며, 경영진과 논의하여 설정할 수 있습니다.
2402.6.3	감사 실무자들은 고위험 문제와 관련하여 조치 마감일 직후 합의된 결과를 확인하여야 하며, 이를 지속적으로 모니터링할 수 있습니다.
2402.6.4	경영진이 약속한 이행 날짜가 다르더라도, 서로 다른 감사에 대한 모든 경영진의 조치 사항은 정기적으로 (예: 분기별) 함께 확인 할 수 있습니다. 또 다른 접근방식은 경영진과 합의한 마감일자에 때라 개별 경영진의 조치 사항을 확인하는 것입니다.

2402.7 사후 활동 성격 및 범위

2402.7.1	일반적으로 피감인에게는 권장사항을 이행하기 위해 취한 조치의 세부사항을 제공할 수 있는 기간이 제공됩니다.
2402.7.2	수행된 조치를 상세히 설명하는 경영진의 대응은 가능하면 원래 검토를 수행한 감사 실무자에 의해 평가되어야 합니다. 가능한 경우, 수행된 조치의 감사 증거를 확보해야 합니다.
2402.7.3	경영진이 권장사항을 이행하기 위해 취한 조치에 대한 정보를 제공하였으나 감사 실무자가 제공된 정보나 수행된 조치의 효과성에 대해 의심을 가질 경우, 추가 사후 활동을 마무리하기 전에 적절한 테스트 또는 기타 감사 절차를 수행하여 실제 위치나 상태를 확인해야 합니다.
2402.7.4	사후 활동의 일환으로, 감사 실무자들은 아직 이행되지 않은 권장사항이 여전히 관련성이 있거나 더 중요성을 가지는지 평가해야 합니다. 감사 실무자들은 특정 권장사항의 이행이 더 이상 적절하지 않다고 결정할 수 있습니다. 이것은 애플리케이션 시스템이 변경된 경우, 보완통제가 구현된 경우, 또는 원래 위험을 효과적으로 제거하거나 상당히 줄이는 방법으로 비즈니스 목표 또는 우선순위가 변경된 경우 발생할 수 있습니다. 마찬가지로, IT 환경의 변화는 이전 관찰의 영향 범위와 그 해결책에 대한 필요성을 증가시킬 수 있습니다.
2402.7.5	중대하거나 중요한 조치의 이행을 확인하기 위해 사후 업무 일정을 계획해야 할 수 있습니다.
2402.7.6	만족스럽지 않은 경영진 대응이나 조치에 대한 감사 실무자의 의견은 적절한 수준의 경영진에게 전달되어야 합니다.

2402.8 사후 활동 연기

2402.8.1	감사 실무자들은 업무 작업 일정 수립의 한 부분으로서 사후 활동 일정을 수립하여야 합니다. 사후 활동의 일정은 관련된 위험과 노출 정도와 시정조치를 이행하는 데 필요한 시간과 난이도에 기반해야 합니다.
2402.8.2	감사 실무자들이 경영진의 구두 또는 서면 대응으로 판단 할 때 이미 취한 조치가 업무 관측 또는 권장사항의 상대적 중요성과 비교 검토했을 때 충분하다고 보는 경우가 있습니다. 이러한 경우, 실제 사후 검증 활동은 관련 시스템 또는 문제를 다루는 다음 업무의 일환으로 수행될 수 있습니다.

2402.9 사후 대응 양식

2402.9.1	서면 대응이 사후 조치와 진행 과정에 대한 경영진의 책임을 강화하고 확인하는 데 도움을 주기 때문에 경영진의 사후 대응을 가장 효과적으로 받는 방법은 서면 형태입니다. 또한 서면 대응은 조치, 책임 그리고 현재 상태에 대한 정확한 기록을 보장합니다. 감사 실무자들은 구두 대응을 받고 기록할 수 있으며 가능한 경우 경영진의 승인을 받습니다. 조치 또는 권장사항 이행의 증명서가 대응과 함께 제공될 수 있습니다.
2402.9.2	실무자들은 특히 고위험 문제 및 리드 타임이 긴 시정조치와 관련하여 경영진이 진행한 상황을 평가하기 위해 합의된 조치를 이행할 책임이 있는 경영진으로부터 주기적인 업데이트를 요청하거나 받을 수 있습니다.

2402.10 외부 감사 권장사항에 대한 감사 실무자의 사후 활동

2402.10.1	감사 업무의 범위와 기간에 따라, 그리고 관련 IT 감사 표준에 따라, 외부 감사 실무자들은 내부 감사 실무자들에 의존하여 합의한 권장사항에 대해 사후 조치를 취할 수 있습니다. 사후 조치에 대한 책임은 감사 헌장 또는 계약서에서 결정할 수 있습니다.

2402.11 사후 활동 보고

2402.11.1	합의되었지만 이행되지 않은 권장사항 등 감사 업무 보고서에서 생성되는 합의된 시정조치의 상태에 대한 보고서가 적절한 수준의 경영진 및 거버넌스 책임자(예: 감사 위원회)에 제시되어야 합니다.
2402.11.2	후속 감사 업무 중 실무자들이 경영진이 "이행됨"으로 보호한 시정조치가 실제로는 이행되지 않았음을 알게 될 경우, 실무자들은 그 상태를 적절한 수준의 경영진 및 거버넌스 책임자에게 알려야 합니다. 해당되는 경우, 실무자들은 현재 시정조치 계획 및 계획된 이행 날짜를 얻어야 합니다.
2402.11.3	합의된 시정조치가 모두 이행되었으면, 이행되었거나 완료된 모든 조치에 대해 자세히 기술하는 보고서를 경영진 및 거버넌스 책임자에게 전달할 수 있습니다.

표준 1402 및 지침 2402를 위한 COBIT® 2019 연결

COBIT 2019 거버넌스 및 관리 목표	목적
EDM01 거버넌스 프레임워크 설정 및 유지보수 보장	기업 거버넌스 접근방식에 통합되고 조정된 일관된 접근방식을 제공합니다. I&T 관련 결정은 기업의 전략 및 목표에 따라 이루어지고 원하는 가치가 실현됩니다. 이를 위해, I&T 관련 프로세스가 효과적이고 투명하게 감독되고, 법적, 계약적, 규제적 요구사항을 준수하는지, 그리고 이사회 구성원에 대한 거버넌스 요구사항이 충족되는지 확인합니다.
EDM02 이익 제공 보장	I&T 지원 이니셔티브, 서비스 및 자산으로 최적의 가치 확보, 솔루션 및 서비스의 비용 효율적인 제공, 비즈니스 요구가 효과적이고 효율적으로 지원될 수 있도록 비용 및 가능한 이점에 대한 신뢰할 수 있고 정확한 그림.
EDM03 위험 최적화에 대한 보장	I&T 관련 기업 위험이 기업의 위험 수용범위 및 위험내성을 초과하지 않고, 기업 가치에 대한 I&T 위험의 영향이 식별되어 관리되고, 규정 준수 실패 가능성을 최소화합니다.
MEA03 외부 요건 준수 관리	기업에 적용되는 모든 외부 요건을 준수하도록 합니다.
MEA04 보증 관리	조직이 효율적이고 효과적인 보증 계획을 설계 및 개발하여, 잘 수용된 보증 접근법에 기초한 로드맵으로 보증 검토를 감사계획, 감사범위 설정, 감사 실행 및 사후 조치하는 과정을 안내할 수 있도록 합니다.

부록 A: 관련 표준 및 표준별 지침

표준	관련 표준	관련 지침
1001 감사 헌장	표준 1001과 관련된 표준 없음	• 지침 2001 감사 헌장
1002 조직의 독립성	표준 1002와 관련된 표준 없음	• 지침 2002 조직의 독립성
1003 감사자 객관성	표준 1003과 관련된 표준 없음	• 지침 2003 감사 객관성
1004 합리적 기대	표준 1004와 관련된 표준 없음	• 지침 2004 합리적 기대
1005 정당한 주의의무	표준 1005와 관련된 표준 없음	• 지침 2005 정당한 주의의무
1006 숙련성	표준 1006과 관련된 표준 없음	• 지침 2006 숙련성
1007 의견 표명	표준 1007과 관련된 표준 없음	• 지침 2007 의견 표명
1008 기준	표준 1008과 관련된 표준 없음	• 지침 2008 기준
1201 계획 수립 시 위험 평가	표준 1201과 관련된 표준 없음	• 지침 2201 계획 수립 시 위험 평가
1202 감사 스케줄링	표준 1202와 관련된 표준 없음	• 지침 2202 감사 스케줄링
1203 업무 계획	표준 1203과 관련된 표준 없음	• 지침 2203 업무 계획
1204 수행 및 감독	• 표준 1005 정당한 주의의무 • 표준 1205 증거 • 표준 1401 보고	• 지침 2204 수행 및 감독 • 지침 2201 계획 수립 시 위험 평가
1205 증거	표준 1205와 관련된 표준 없음	• 지침 2205 증거
1206 다른 전문가의 작업 사용	표준 1206과 관련된 표준 없음	• 지침 2206 다른 전문가의 작업 사용
1207 부정 및 불법 행위	• 표준 1008 기준 • 표준 1201 계획 수립 시 위험 평가 • 표준 1205 증거	• 지침 2206 다른 전문가의 작업 사용 • 지침 2207 부정 및 불법 행위
1401 보고	표준 1401과 관련된 표준 없음	• 지침 2401 보고
1402 사후 활동	표준 1402와 관련된 표준 없음	• 지침 2402 사후 활동

이 페이지는 의도적으로 비워둠

부록 B: 지침별 관련 표준

지침	관련 표준
2001 감사 헌장	• 1001 감사 헌장 • 1002 조직의 독립성 • 1003 감사자 객관성
2002 조직의 독립성	• 1001 감사 헌장 • 1002 조직의 독립성 • 1003 감사자 객관성 • 1004 합리적 기대 • 1006 숙련성
2003 감사 또는 객관성	• 1001 감사 헌장 • 1002 조직의 독립성 • 1003 감사자 객관성 • 1005 정당한 주의의무
2004 합리적 기대	• 1001 감사 헌장 • 1004 합리적 기대
2005 정당한 주의의무	• 1002 조직의 독립성 • 1003 감사자 객관성 • 1005 정당한 주의의무 • 1006 숙련성 • 1205 증거
2006 숙련성	• 1005 정당한 주의의무 • 1006 숙련성 • 1203 업무 계획 • 1204 수행 및 감독
2007 의견 표명	• 1007 의견 표명 • 1008 기준 • 1206 다른 전문가의 작업 사용 • 1401 보고
2008 기준	• 1007 의견 표명 • 1008 기준
2201 계획 수립 시 위험 평가	• 1201 계획 수립 시 위험 평가 • 1203 업무 계획 • 1204 수행 및 감독 • 1207 부정 및 불법 행위

지침	관련 표준
2202 감사 스케줄링	• 1201 계획 수립 시 위험 평가 • 1203 업무 계획 • 1204 수행 및 감독 • 1207 부정 및 불법 행위
2203 업무 계획	• 1201 계획 수립 시 위험 평가 • 1203 업무 계획 • 1204 수행 및 감독
2204 수행 및 감독	• 1005 정당한 주의의무 • 1006 숙련성 • 1203 업무 계획 • 1204 수행 및 감독 • 1205 증거 • 1401 보고

부록 C: 용어 및 정의

감

감사 계획 — 1. 의견을 수립하고, 적절한 감사 증거를 충분히 확보하기 위해 감사팀원이 수행할 감사 절차의 성격, 시기 및 범위를 포함하는 계획.

범위 참고: 감사 대상 영역, 계획된 작업 유형, 작업의 전체 목적 및 범위, 그리고 예산, 자원 할당, 일정 날짜, 보고서 유형 및 대상 사용자 및 작업의 다른 일반적인 측면과 같은 주제를 포함합니다.

2. 특정 기간에 수행될 감사 작업에 대한 전체 설명.

감사 업무 — 감사, 통제 자가 평가 검토, 사기 행위 검사 또는 컨설팅 등 구체적인 감사 과제, 작업 또는 검토 활동 감사 활동에는 구체적인 관련 목표 달성을 위한 복합적인 작업이나 활동이 해당될 수 있음

감사 위험 — 감사 결과를 바탕으로 부정확한 결론에 도달할 수 있는 위험.

범위 참고: 감사 위험의 3가지 요소:
- 통제 위험
- 적발 위험
- 고유 위험

감사 프로그램 — 감사를 완료하기 위해 수행해야 하는 감사 절차 및 지침의 단계별 집합.

감사 헌장 — 내부 감사 활동의 목적, 권한, 책임이 정의되어 있고 거버넌스 책임자가 승인한 문서.

범위 참고: 헌장의 역할:
- 내부 감사 담당자의 기업 내 직책 수립
- IS 감사 및 보증 업무 수행과 관련된 기록, 인력 및 물리적 속성에 대한 액세스 허가
- 감사 담당자의 활동 범위 정의

감사자 의견 — 감사 범위, 보고서 생성에 사용된 절차, 결과상 감사 기준이 충족되었음을 뒷받침하는지 여부가 설명되어 있고 IS 감사 또는 보증 전문가가 작성한 공식 진술서.

범위 참고: 의견의 유형:
- **적정 의견** — 예외 없음 또는 기록된 예외 없음이 중요 결함으로 귀결되지 않음.
- **한정 의견** — 예외가 중요 결함(중요 취약성은 아님)으로 귀결됨.
- **부적정 의견** — 1개 이상의 중요 결함이 중요 취약성으로 귀결됨.

객

객관성 — 공정하게 판단력을 행사하고 의견을 표현하며 권고 사항을 제시할 수 있는 능력

고

고유 위험 — 경영진이 취했거나 취할 수 있는 조치를 감안하지 않은 위험 수준 또는 노출(예: 통제책 이행).

관

관련 정보 — 통제와 관련하여, 기초 통제 또는 통제 요소 운영에 관해 평가자에게 의미 있는 내용을 내포하는 정보. 통제의 운영이 가장 적합함을 직접 확정하는 정보. 통제 운영과 간접적으로 연관된 정보도 해당될 수 있지만, 직접 정보보다는 적절성이 낮음.

범위 참고: COBIT 5 정보 품질 목표를 참조하십시오.

기

기술서 — 경영진이 전문가에게 제출한 서명 또는 구두 진술서로, 경영진은 경영진이 잘 아는 바로, 현재 또는 미래 사실(예: 프로세스, 시스템, 절차, 정책)이 특정 상태에 있거나 있을 예정임을 선언합니다.

기준 — 주제 사안을 측정하고 제시하는 데 사용되고 IS 감사인이 주제 사안을 평가할 때 바탕으로 하는 표준 및 벤치마크

범위 참고: 기준의 요건:
- **객관성** — 편향적이지 않음
- **측정 가능** — 일관된 측정을 위해 제공됨
- **완전성** — 결론 도달을 위한 모든 적절한 요소가 포함됨
- **관련성** — 주제 사안과 관련됨

증명 업무 시, 주제 사안에 관한 경영진의 서면 의견 표명을 바탕으로 한 벤치마크가 평가될 수 있습니다. 실무자는 적합한 기준을 지칭함으로써 주제 사안에 관한 결론을 형성합니다.

다

다른 전문가 — 기업 내외부에 속한 다른 전문가란:
- 외부 회사 소속의 IT 감사자
- 경영 컨설턴트
- 최고 경영진 또는 팀에 의해 지명된 업무 분야의 전문가

독

독립성 — 자체 통제 및 이해 충돌 및 부당한 위압으로부터 자유로움. IT 감사자는 자유롭게 스스로 결정을 내리고 감사 받는 조직이나 그 조직원(관리자 및 직원)으로부터 영향을 받지 않아야 합니다.

무

무결성 — 부적절한 정보 수정이나 파기로부터 보호하며, 정보 부인 방지 및 인증을 보장합니다.

보

보증 업무 — 기업의 위험 관리, 통제 또는 거버넌스 절차를 제공할 목적으로 증거를 객관적으로 검사하는 행위

범위 참고: 예로는 금융, 성과, 준수, 시스템 보안 업무 등이 있습니다.

부

부정 — 수립된 경영진 정책 또는 규제 요건을 위반하는 행위. 부정은 중과실 또는 비의도적인 불법 행위로서 감사 중인 분야 또는 기업에 관한 정보의 고의적인 문서상의 오류나 누락으로 구성될 수 있습니다.

사

사고의 객관성 — 개인이 무결성, 객관성 및 전문가적 의구심의 행사에 입각하여 행동할 수 있도록, 전문적 판단력을 해치는 영향력으로부터 영향을 받지 않고 결론을 표현하는 것을 허하는 마음 상태.

사후 활동 — 경영진이 결함을 해결하기 위해 적절한 시정조치를 취했는지 여부를 판별하는 활동.

설

설계 효과성 — 회사의 통제장치가 효과적으로 통제를 수행하기 위한 필요한 권한과 역량을 가진 사람에 의해 규정된 대로 작동될 경우, 그리고 이러한 통제장치가 회사의 통제 목적을 충족시키고 재무제표에 실질적인 표기 오류를 초래할 수 있는 오류나 사기를 효과적으로 방지하거나 탐지할 수 있으면, 효과적으로 설계되었다고 간주됩니다.

상장기업 회계감독 위원회(PCAOB), 감사 표준 번호. 2201, "재무제표 감사와 통합된 재무 보고에 대한 내부 통제 감사", 2007년 11월 15일, 섹션 42 (*https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx*)를 참조하십시오.

손

손상 — 감사 목표를 수행하기 위한 능력이 약화 또는 감소되는 상태

범위 참고: 조직상 독립성 및 개별 객관성이 손상되는 행위에는 개인적 이해 상충, 범주 제한, 기록, 직원, 장비, 시설 액세스 제한, 자원 제한(자금, 인력 등)이 있을 수 있음.

신

신뢰 가능한 정보 — 정확하고 확인 가능하며 객관적인 출처에서 발생한 정보.

범위 참고: COBIT 5 정보 품질 목표를 참조하십시오.

실

실증 테스팅 — 감사 기간 중에 활동이나 트랜잭션의 완전성, 정확성 또는 존재 여부에 대한 감사 증거를 확보하는 행위.

외

외관상 객관성 — 중요성이 높아 합리적이고 정보를 보유한 제삼자가 구체적인 사실 및 상황을 모두 고려했을 때 법인, 감사 담당자 또는 감사 팀원의 무결성, 객관성 또는 전문가적 의구심이 손상되었다고 결론을 내릴 가능성이 있는 사실 및 상황을 피하는 행위.

운

운영 효과성 — 통제가 설계된 대로 운영되고 통제를 수행하는 사람이 통제를 효과적으로 수행하기에 필요한 권한과 역량을 가지고 있으면, 그 통제는 효과적으로 운영되고 있는 것으로 간주됩니다.

상장기업 회계감독 위원회(PCAOB), 감사 표준 번호 2201, "AS 2201: 재무제표 감사와 통합된 재무 보고에 대한 내부 통제 감사", 2007년 11월 15일 (*https://pcaobus.org/Standards/Auditing/Pages/AS2201.aspx*)을 참조하십시오.

위

위험 평가 — 위험과 위험의 잠재적 영향을 식별하고 평가하는 데 사용되는 프로세스

범위 참고: 위험 평가는 IS 연간 감사 계획서에 포함하기 위해 최고의 위험, 취약성, 기업으로의 노출을 나타내는 항목이나 분야를 파악하는 데 사용됨.

프로젝트 이행 및 프로젝트 수익 위험을 관리할 때도 사용됨.

위협 — 유해를 입힐 수 있는 방식으로 자산에 대해 행동할 수 있는 것(예: 객체, 물질, 인간)

범위 참고: 원하지 않는 사고의 잠재적 원인 (ISO/IEC 13335)

의

의견 표명 — 경영진이 만든 주제 사안에 관한 공식 선언 또는 선언의 집합

범위 참고: 의견 표명은 보통 서면 형태여야 하고, 일반적으로 주제 사안이나 주제 사안에 연관된 절차에 관한 구체적인 특성 목록이 포함됨.

잔

잔여 위험 — 경영진이 위험 대응을 이행한 후 남은 위험

적

적발 위험 — 오류 또는 사기를 시기적절하게 탐지하는 기업의 내부 통제장치 장애로 인해 자산이 손실/훼손되거나 재무제표가 실질적으로 잘못 표시되는 위험

적절한 증거 — 증거 품질에 대한 측정

적합한 정보 — 적절성(예: 의도된 목적과 부합하는가), 신뢰성(예: 정확하고 확인 가능하며 객관적인 출처에서 발생), 적기성(예: 적합한 일정 내에서 생성 및 사용됨)을 갖춘 정보.

범위 참고: COBIT 5 정보 품질 목표를 참조하십시오.

전

전문가 능력 — 입증된 능력 수준. 종종 관련 전문 기관이 발행한 적격성 및 해당 기관의 관행 및 표준 규정 준수와 연결됨.

전문가 판단 — IS 감사 및 보증 업무 상황에 적합한 일련의 조치에 대해 정보에 입각한 결정을 내리는 데 관련 지식과 경험 적용

전문가적 의구심 — 문제를 제기하는 태도, 감사 증거의 중대한 평가 등에 해당되는 태도.

범위 참고: 출처: American Institute of Certified Public Accountants (AICPA) AU 230.07

주

주제 사안 — IS 감사자의 보고서 및 관련 절차를 따르는 구체적인 정보. 이것은 내부 통제의 설계 또는 작업과 개인정보 보호 관행 또는 표준이나 지정된 법과 규정(활동 영역) 준수와 같은 것을 포함할 수 있습니다.

중

중요 결함 — 중요한 약점보다는 덜 심각하지만, 감독 책임을 지는 사람의 주의를 끌 만큼은 중요한 내부 통제의 결함 또는 결함의 조합.

범위 참고: 중요 취약성은 예방되거나 감지되지 않은 바람직하지 않은 이벤트가 원격적으로 2회 이상 발생할 수 있는 중요 결함이나 중요 결함의 조합을 의미합니다.

중요 취약성 — 중요한 문서상의 오류가 적시에 예방 또는 적발될 수 없다는 합리적인 가능성이 존재하는 경우 등 내부 통제에 존재하는 결함 또는 결함의 조합. 통제의 부재로 인해 통제 목적의 달성에 대한 합리적 확신을 제공할 수 없는 경우, 통제의 취약성을 '중요한 것'으로 간주함. 중요로 분류된 약점은 다음 내용을 내포합니다.

- 통제가 없음 및/또는 통제가 사용되지 않음 및/또는 통제가 적절하지 않음
- 단계적으로 확대됨

중요도와 IS 감사 및 보증 전문가가 수용할 수 있는 감사 위험성 사이에는 서로 반대 관계가 있습니다. 즉, 중요도 수준이 높아질수록 감사 위험성의 수용 가능성은 낮아지고, 반대로 수준이 낮아질수록 수용 가능성이 높아집니다.

중요성 — 감사 대상의 기능에 대해 미치는 영향과 관련한 정보 항목의 중요성에 관한 감사 개념. 기업 전체의 문맥에서 상대적 중요성 또는 특정 사안의 중요도를 지칭한 표현.

증

증명 — IT 감사자가 특정 주제 사안에 대한 경영진의 의견 표명이나 주제 사안을 직접 살펴보기 위해 참여하는 업무.

충

충분한 정보 — 정보가 충분한 시기는 평가자가 합리적인 결론을 도출할 수 있을 정도로 충분한 내용이 수집되었을 때임. 그러나 정보가 충분하기 위해서는 먼저 적합해야 함.

범위 참고: COBIT 5 정보 품질 목표를 참조하십시오.

충분한 증거 — 감사 증거 수량에 대한 측정. 감사 목적 및 범위에 대한 모든 중요 문의를 뒷받침해야 함.

범위 참고: 증거를 참조하십시오.

통

통제 위험 — 내부 통제의 설계 및/또는 구현 부재 또는 비효율성으로 인한 자산이 손실/훼손되었거나 재무제표가 실질적으로 잘못 표기되는 위험

합

합리적 확신 — 보장 수준에는 약간 못미치지만, 통제 비용과 달성될 수 있는 편익을 고려할 때 적절하다고 간주됩니다.