ITAF™

3-тє видання

Основні положення професійної практики аудиту та підтвердження довіри до ІС

ISACA®

Trust in, and value from, information systems

Про ISACA®

Об'єднуючи більше 115 000 членів у 180 країнах світу, ISACA[1] (www.isaca.org) допомагає лідерам у сфері бізнесу та інформаційних технологій забезпечувати корисність та довіру до інформації та інформаційних систем. Із часу заснування асоціації у 1969 році вона є надійним джерелом знань, стандартів, співробітництва та підвищення кваліфікації для фахівців у галузі аудиту, підтвердження достовірності, безпеки, управління ризиками, конфіденційності та управління інформаційними системами. ISACA пропонує фахівцям із кібербезпеки широкий набір ресурсів Cybersecurity Nexus™ та бізнес-архітектуру COBIT®[2], яка допомагає організаціям в управлінні та контролі за інформацією та технологіями. Асоціація також розвиває та підтверджує найбільш важливі для бізнесу навички та знання, поширюючи сертифікації,що визнаються у міжнародному масштабі: CISA®[3], CISM®[4], CGEIT®[5] та CRISC™[6]. ISACA має понад 200 відділень по всьому світу.

Обмеження відповідальності

ISACA розробила та опублікувала *ITAF™[7]: Основні положення професійної практики аудиту та підтвердження довіри до ІС. 3-тє видання* (далі – Твір) насамперед як освітній ресурс для фахівців з підтвердження довіри. Асоціація не стверджує, що використання Твору гарантуватиме отримання успішних результатів. Твір не слід розглядати як такий, що містить усю необхідну інформацію, процедури та тести; також не виключається, що інша інформація, процедури та тести можуть зумовити отримання аналогічних результатів. При визначенні доцільності застосування будь-якої інформації, процедури або тесту фахівці з підтвердження довіри повинні керуватися власними професійними судженнями щодо конкретних обставин в умовах існуючих систем або середовища інформаційних технологій.

Disclaimer

ISACA has designed and created *ITAF™: A Professional Practices Framework for IS Audit / Assurance, 3rd Edition* (the 'Work') primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Правові застереження

Reservation of Rights

Положення про якість

Цей Твір перекладено українською мовою з англійської версії *ITAF™: A Professional Practices Framework for IS Audit / Assurance, 3rd Edition* Київським відділенням ISACA® з дозволу ISACA®. За точність і достовірність перекладу відповідальність несе виключно Київське відділення ISACA®.

Quality Statement

This Work is translated into Ukrainian from the English language version of *ITAF™: A Professional Practices Framework for IS Audit / Assurance, 3rd Edition* by the ISACA® Kyiv Chapter with the permission of ISACA®. The ISACA® Kyiv Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

---

[1] ISACA (Information Systems Audit and Control Association) – Асоціація аудиту та контролю інформаційних систем

[2] COBIT® (Control Objectives for Information and Related Technologies) – «Цілі контролю для інформаційних та суміжних технологій»

[3] CISA® (Certified Information Systems Auditor) – Сертифікований аудитор інформаційних систем

[4] CISM® (Certified Information Security Manager) – Сертифікований менеджер з інформаційної безпеки

[5] CGEIT® (Certified in the Governance of Enterprise IT) – Сертифікований фахівець з управління корпоративними IT

[6] CRISC™ (Certified in Risk and Information Systems Control) – Сертифікований фахівець у галузі ризиків та контролю інформаційних систем

[7] ITAF™ (IT Assurance Framework) – «Основні положення професійної практики аудиту та підтвердження довіри до IT»

ISACA®
Роллінг-Медоуз, Іллінойс, США, 60008
Телефон: +1 847 253 1545
Факс: +1 847 253 1443
Електронна пошта: Info@isaca.org
Веб-сайт: www.isaca.org

Залишити коментар: www.isaca.org/ITAF
Приєднатися до Центру знань ISACA: www.isaca.org/knowledge-center
Стежити за ISACA у Twitter: https://twitter.com/ISACANews
Приєднатися до ISACA в LinkedIn: ISACA (Official), http://linkd.in/ISACAOfficial
Уподобати ISACA у Facebook: www.facebook.com/ISACAHQ

Подяка

ISACA висловлює подяку:

Раді директорів ISACA

Тоні Хейс (Tony Hayes), CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, уряд Квінсленду, Австралія, міжнародний президент
Алан Бордман (Allan Boardman), CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, банківський холдинг «Морган Стенлі» (Morgan Stanley), Великобританія, віце-президент
Хуан Луїс Карсель (Juan Luis Carselle), CISA, CGEIT, CRISC, мережа універсальних магазинів «Вол-Март» (Wal-Mart), Мексика, віце-президент
Рамзес Галлего (Ramses Gallego), CISM, CGEIT, CCSK, CISSP, SCPM, кваліфікація «Чорний пояс» по системі «Шість сигма», комп'ютерна компанія «Делл» (Dell), Іспанія, віце-президент
Тереза Графенштайн (Theresa Grafenstine), CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, Палата представників США, США, віце-президент
Віттал Радж (Vittal Raj), CISA, CISM, CGEIT, CFE, CIA, CISSP, FCA, компанія «Кумар енд Радж» (Kumar & Raj), Індія, віце-президент
Джефф Співі (Jeff Spivey), CRISC, CPP, PSP, корпорація «Сек'юріті Ріск Менеджмент Інк.» (Security Risk Management Inc.), США, віце-президент
Марк Вael (Marc Vael), д. філос. н., CISA, CISM, CGEIT, CRISC, CISSP, компанія «Вельюенду» (Valuendo), Бельгія, віце-президент
Грегорі Т. Грочолскі (Gregory T. Grocholski), CISA, хімічна компанія «Зе Дау Кемікал Ко.» (The Dow Chemical Co.), США, колишній міжнародний президент
Кеннет Л. Вандер Уал (Kenneth L. Vander Wal), CISA, CPA, партнерство з обмеженою відповідальністю «Ернст енд Янг» (Ernst & Young LLP), пенсіонер, США, колишній міжнародний президент
Крістос К. Дімітріадіс (Christos K. Dimitriadis), д. філос. н., CISA, CISM, CRISC, AT «ІНТРАЛОТ» (INTRALOT S. A.), Греція, директор
Крістен МакКейб (Krysten McCabe), CISA, компанія «Зе Хоум Діпо» (The Home Depot), США, директор
Джо Стюарт-Реттрей (Jo Stewart-Rattray), CISA, CISM, CGEIT, CRISC, CSEPS, консультативна практика «БіАрЕм Холдіч» (BRM Holdich), Австралія, директор

Раді з питань атестування та управління кар'єрним ростом

Алан Бордман (Allan Boardman), CISA, CISM, CGEIT, CRISC, ACA, CA (SA), CISSP, банківський холдинг «Морган Стенлі» (Morgan Stanley), Великобританія, голова
Бернард Баттістін (Bernard Battistin), CISA, CMA, Управління Генерального аудитора Канади, Канада
Річард Брісбойс (Richard Brisebois), CISA, CGA, Канада
Террі Крісман (Terry Chrisman), CGEIT, CRISC, компанія споживчого кредитування «Джіл Мані» (GE Money), США
Ерік Фріболін (Erik Friebolin), CISA, CISM, CRISC, CISSP, PCI-QSA, бібліотека інфраструктури інформаційних технологій «АйТіАйЕл» (ITIL), США
Френк Нільсен (Frank Nielsen), CISA, CGEIT, CCSA,CIA, фінансова група «Нордеа» (Nordea), Данія
Хітоші Ота (Hitoshi Ota), CISA, CISM, CGEIT, CRISC, CIA, банк «Мідзухо Корпорейт Бенк» (Mizuho Corporate Bank), Японія
Кармен Озорес Фернандес (Carmen Ozores Fernandes), CISA, CRISC, Бразилія
Стівен Е. Сайзмо (Steven E. Sizemore), CISA, CIA, CGAP, Комісія з питань охорони здоров'я та соціального забезпечення населення Техасу, США

Комітету з питань професійних стандартів та управління кар'єрним ростом

Стівен Е. Сайзмо (Steven E. Sizemore), CISA, CIA, CGAP, Комісія з питань охорони здоров'я та соціального забезпечення населення Техасу, США, голова
Крістофер Найджел Купер (Christopher Nigel Cooper), CISM, CITP, FBCS, член Інституту професіоналів з інформаційної безпеки, компанія «ЕйчПі Ентерпрайз Сек'юріті Сервісіз» (HP Enterprises Security Services), Великобританія
Рональд Е. Френкі (Ronald E. Franke), CISA, CRISC, CFE, CIA, CICA, компанія «Маєрз енд Штауффер» (Myers and Stauffer LLC), США
Елісдеа МакКензі (Alisdair McKenzie), CISA, CISSP, ITCP, компанія «Ай Ес Ешуеренс Сервісіз» (I S Assurance Services), Нова Зеландія
Камесвара Рао Намудурі (Kameswara Rao Namuduri), д. філос. н., CISA, CISM, CISSP, Університет Північного Техасу, США
Катсумі Сакагава (Katsumi Sakagawa), CISA, CRISC, PMP, публічна компанія «ДжейАйІСі Ко. Лтд.» (JIEC Co. Ltd.), Японія
Ієн Сендерсон (Ian Sanderson), CISA, CRISC, FCA, HATO, Бельгія
Тімоті Сміт (Timothy Smith), CISA, CISSP, CPA, організація «ЕлПіЕл Файненшиал» (LPL Financial), США
Тодд Вайманн (Todd Weinman), CPS, компанія «Зе Вайманн Груп» (The Weinman Group), США

Технічним рецензентам українського перекладу

Гліб Пахаренко, CISA, CISSP

Олексій Довидьков, д. філос. н.

Олексій Кудряшов, MBA, CPMP IPMA (рівень C), Спільне британо-українське підприємство «Полтавська газонафтова компанія»

Дем'ян Островський, ЗАТ «БеСТ» (CJSC "BeST"), «ЛайфТек» (LifeTech), «Турксел Груп» (Turkcell Group)

Ірина Івченко, «ЕсАйСентер» (SICenter)

Олексій Янковський, «Груп-ДФ» (Group-DF)

Андрій Красний, «Делойт» (Delloite)

Перекладачу на українську мову

Тетяна Мерега

Зміст

Вступ

ITAF – це вичерпна еталонна модель використання кращих практик, яка:
- встановлює стандарти, що описують ролі та обов'язки фахівців з аудиту та підтвердження довіри до ІС; їх знання та навички; ретельність; вимоги до проведення аудиту та звітності;
- визначає терміни та поняття, специфічні для сфери підтвердження довіри до ІС;
- описує принципи, інструменти і методики планування, розробки, проведення та звітування за результатами завдань з аудиту та підтвердження довіри до ІС.

ITAF орієнтується на матеріали ISACA і є єдиним джерелом, до якого можуть звертатися фахівці з аудиту та підтвердження довіри до ІС за настановами, для дослідження політик і процедур, отримання програм аудиту та підтвердження довіри, а також формування ефективних звітів.

ITAF. 2-ге видання об'єднує стандарти та настанови ISACA щодо аудиту та підтвердження довіри до ІС, діючі з 1 листопада 2013 року. *ITAF. 3-тє видання* містить настанови, діючі з 1 вересня 2014 року. Як тільки будуть розроблені та видані нові настанови, вони будуть внесені до основних положень.

При підготовці стандартів і настанов з аудиту та підтвердження довіри до ІС до консультацій залучали Комітет ISACA з професійних стандартів та управління кар'єрним ростом. Перед виданням будь-якого документу на міжнародному рівні публікується попередній проект для отримання коментарів від широкого загалу. Попередній проект документу та супровідна онлайн-анкета будуть доступні за посиланням: www.isaca.org/standardexposure. Окрім того, коментарі можна надсилати електронною поштою до уваги директора з розвитку професійних стандартів на таку адресу: standards@isaca.org. Коментарі щодо українського перекладу цього документу можна надсилати на адресу: office@isaca.org.ua.

Питання, які часто задають

- **До кого застосовується ITAF?** ITAF застосовується до осіб, які є фахівцями з аудиту та підтвердження довіри до ІС і залучаються до підтвердження довіри до складових прикладних програм та інфраструктури ІС. Однак, ці стандарти, настанови, інструментарій і методики було розроблено таким чином, щоб їх могла з користю застосовувати також ширша аудиторія, у тому числі користувачі звітів аудиту та підтвердження довіри до ІС.

- **Коли слід використовувати ITAF?** Застосування основних положень є необхідною передумовою проведення аудиту та підтвердження довіри до ІС. Стандарти носять обов'язковий характер. Настанови, інструментарій і методики розроблено для надання необов'язкової допомоги у виконанні завдань з підтвердження довіри.

- **Де слід використовувати стандарти аудиту та підтвердження довіри до ІС ITAF і пов'язані з ними настанови?** Дизайн ITAF передбачає, що перед фахівцями з аудиту та підтвердження довіри до ІС висуватимуться різні вимоги і типи завдань (від управління аудитом, спрямованим на ІС, до участі у фінансовому чи операційному аудиті). ITAF застосовується до всіх офіційних аудитів ІС та завдань з оцінювання.

- **Чи охоплює ITAF вимоги до консалтингової / консультаційної діяльності?** Окрім оцінювання, фахівці з аудиту та підтвердження довіри до ІС часто виконують для своїх роботодавців чи від імені клієнтів консалтингові та консультаційні завдання. Як правило, ці завдання полягають в оцінці певної сфери; виявленні проблем, ускладнень і вразливих місць; а також у розробці рекомендацій. З різних причин, включаючи характер роботи, обсяг завдань, незалежність та рівень тестування, така робота не вважається аудитом і, відповідно, фахівці з аудиту та підтвердження довіри до ІС не формують офіційного аудиторського звіту. Стандарти ITAF не розроблялись для того, щоб відповідати особливим вимогам такої консалтингової / консультаційної діяльності.

Організація

Стандарти аудиту та підтвердження довіри до ІС ITAF поділяються на три категорії:
- **загальні стандарти (серії 1000)** – це основні принципи, згідно з якими працюють фахівці у галузі підтвердження довіри до ІС. Вони застосовуються при виконанні усіх завдань та описують етику, незалежність, об'єктивність, належну професійну ретельність, а також знання, компетенцію та навички фахівців з аудиту та підтвердження довіри до ІС;
- **стандарти виконання (серії 1200)** регулюють виконання таких завдань, як планування та нагляд, оцінювання обсягу завдань, управління ризиками та суттєвість, мобілізація ресурсів, управління завданнями та наглядом, докази аудиту та підтвердження довіри, а також застосування професійних суджень і забезпечення належної професійної ретельності;

• **стандарти звітування (серії 1400)** описують типи звітів, способи звітування та інформацію, що надається.

Настанови з аудиту та підтвердження довіри до ІС ITAF забезпечують фахівців з аудиту та підтвердження довіри до ІС інформацією та вказівками у сфері аудиту та підтвердження довіри до ІС. Відповідно до трьох вищеописаних категорій стандартів настанови зосереджені на різноманітних аудиторських підходах, методиках і супутніх матеріалах для надання допомоги у плануванні, виконанні, оцінюванні, тестуванні та звітуванні щодо процесів ІС і пов'язаних ініціатив з аудиту та підтвердження довіри до ІС. Крім того, настанови допомагають з'ясувати взаємозв'язок між діяльністю та ініціативами організації і тим, що здійснюється за допомогою ІТ.

Настанови з аудиту та підтвердження довіри до ІС ITAF також поділяються на три категорії:
• **загальні настанови (серії 2000)**;
• **настанови виконання (серії 2200)**;
• **настанови звітування (серії 2400)**.

Інструментарій і методики (серії 3000) описують специфічну інформацію щодо різноманітних методик, інструментів і шаблонів, а також рекомендації щодо їх застосування та використання для залучення інформації, наведеної в настановах. Необхідно звернути увагу, що інструментарій і методики можуть бути різної форми, такі як документи для обговорення, технічні рекомендації, білі книги, аудиторські програми та книги, наприклад, видання ISACA про систему SAP, яке описує систему планування ресурсів підприємства (ERP-систему).

Оскільки ITAF було розроблено як документ, що актуалізується, у номерах розділів були навмисно залишені пропуски, куди можна вставити майбутні настанови.

Застосування ITAF

Стандарти завжди носять обов'язковий характер. Термін «повинен» означає «має» Усі відхилення від них необхідно врегулювати до виконання завдань з аудиту та підтвердження довіри до ІС.

Настанови не носять обов'язковий характер, але наполегливо рекомендується їх дотримуватися. Хоча вони дійсно надають фахівцям з аудиту та підтвердження довіри до ІС певний ступінь свободи у їх застосуванні, необхідно, щоб фахівці могли обґрунтувати і виправдати будь-яке значне відхилення від настанов або упущення їх важливих розділів при виконанні завдань з аудиту та підтвердження довіри до ІС. Особливо це стосується тих завдань, які виконуються більше на рівні аудиту ІС. Не у всіх ситуаціях застосовуються усі настанови, але їх завжди треба враховувати.

Інструментарій і методики є додатковими матеріалами та інформацією, що сприяють виконанню настанов. У деяких випадках методики мають альтернативні варіанти або навіть є низкою методик, багато з яких можна застосовувати. Методики слід обирати тільки у випадку їх придатності та відповідності, а також якщо за їх допомогою фахівці з аудиту та підтвердження довіри до ІС отримають доречну, відповідну, об'єктивну та неупереджену інформацію.

Вичерпну інформацію щодо стандартів та настанов з аудиту та підтвердження довіри до ІС ISACA можна отримати за наступним посиланням: www.isaca.org/standards (www.isaca.org.ua).

Процес аудиту ІС або процес підтвердження довіри до ІС передбачає виконання специфічних процедур для забезпечення належного рівня довіри до об'єкта перевірки. Фахівці з аудиту та підтвердження довіри до ІС виконують завдання, які спрямовані на забезпечення довіри на різних рівнях: від обстеження до атестування або екзаменування.

Кожне завдання з аудиту та підтвердження довіри до ІС повинно відповідати встановленим стандартам стосовно того, чи є особи достатньо кваліфікованими для виконання цієї роботи, як виконується робота, яка робота виконується, і яким чином буде проводитися звітування на основі різних характеристик завдання та природи отриманих результатів. Якщо завдання виконується однією особою, необхідно, щоб ця особа володіла навичками та знаннями, потрібними для повного виконання завдання. Якщо завдання виконується більше, ніж однією особою, необхідно, щоб група колективно володіла навичками та знаннями, потрібними для виконання роботи.

Завданням з аудиту та підтвердження довіри до ІС притаманні кілька важливих припущень, у тому числі:
• об'єкт перевірки можна ідентифікувати та піддати аудиту;
• існує висока ймовірність успішного завершення проекту;
• обрані підхід і методика є неупередженими;
• сфера застосування проекту є достатньою для досягнення цілей аудиту та підтвердження довіри до ІС;

• проект завершиться формуванням об'єктивного звіту, який не буде дезінформувати читачів.

Стандарти, видані іншими органами зі стандартизації

Незважаючи на те, що стандарти ITAF забезпечують фахівців з аудиту та підтвердження довіри до ІС необхідними настановами і вказівками, можуть виникати ситуації, коли фахівцям буде необхідно використовувати нормативні документи та стандарти, розроблені іншими організаціями.

Фахівці з аудиту та підтвердження довіри до ІС можуть:
• користуватися стандартами ITAF у поєднанні з професійними стандартами, виданими іншими повноважними органами;
• посилатися у своїх звітах на використання інших стандартів.

У випадку використання фахівцями з аудиту та підтвердження довіри до ІС інших стандартів необхідно впевнитися, що ці стандарти не вступають у конфлікт зі стандартами ITAF.

Якщо фахівці з аудиту та підтвердження довіри до ІС посилаються на відповідність стандартам ITAF, та якщо існують розбіжності між стандартами ITAF та іншими стандартами, при проведенні перевірок та звітуванні результатів фахівці з аудиту та підтвердження довіри до ІС повинні дотримуватись стандартів ITAF як переважаючих, якщо інші стандарти не є регуляторними вимогами.

Терміни та визначення

У цьому документі звичайні слова використовуються у специфічних значеннях. Для того, щоб ці слова та їх контекстуальні значення трактувалися та вживалися правильно в рамках цього документу, на веб-сайті ISACA наводиться повний глосарій термінів: www.isaca.org.ua/itaf_glossary. Такі визначення стосуються найбільш розповсюджених типів завдань, які виконують фахівці з аудиту та підтвердження довіри до ІС. Хоча вони відповідають визначенням AICPA[8] та ISAAB[9], однак, фахівцям слід звертатися до найновіших стандартів з першоджерел, що відносяться до специфічних типів завдань, щоб забезпечити при їх виконанні відповідність найновішим професійним стандартам.

[8] AICPA (American Institute of Certified Public Accountants) – Американський інститут дипломованих громадських бухгалтерів

[9] ISAAB (International Auditing and Assurance Standards Board) – Рада з міжнародних стандартів аудиту та підтвердження довіри

Кодекс професійної етики ISACA

ISACA встановлює цей Кодекс професійної етики, щоб описати професійну та особисту поведінку членів асоціації та / або власників її сертифікатів.

Члени та власники сертифікатів ISACA повинні:
1) сприяти впровадженню та забезпеченню відповідності стандартам і процедурам для ефективного корпоративного управління та управління інформаційними системами і технологіями організації, включаючи аудит, контроль, безпеку та управління ризиками;
2) виконувати свої обов'язки об'єктивно, старанно, з належною професійною ретельністю та згідно з професійними стандартами;
3) працювати у рамках закону в інтересах зацікавлених сторін, дотримуючись високих стандартів поведінки та репутації, не дискредитуючи свою професію або Асоціацію;
4) не розголошувати комерційні таємниці та конфіденційну інформацію, отримані в рамках здійснення діяльності, окрім випадків, коли це вимагається законом. Не використовувати таку інформацію для особистої вигоди та не розкривати її стороннім особам;
5) підтримувати знання у сферах своєї діяльності та братися за виконання тільки таких завдань, які можна завершити за допомогою необхідних навичок, знань і професійної компетентності;
6) інформувати відповідні сторони про результати виконання роботи, у тому числі розкривати їм усі важливі факти, які у разі нерозкриття можуть викривити звіти за результатами діяльності;
7) сприяти професійній освіті зацікавлених сторін, поглиблюючи їхнє розуміння корпоративного управління та управління інформаційними системами і технологіями організації, включаючи аудит, контроль, безпеку та управління ризиками.

Порушення цього Кодексу професійної етики може призвести до розгляду поведінки члена чи власника сертифікату і, врешті, до дисциплінарних заходів.

1. Стандарти аудиту та підтвердження довіри до ІС

Як зазначалось у Вступі, необхідно завжди слідувати усім стандартам ITAF: загальним, виконання та звітування. Окрім того, ці стандарти містять ключові аспекти, розроблені для сприяння діяльності фахівців з аудиту та підтвердження довіри до ІС; саме тому, інформація, якої необхідно дотримуватися в обов'язковому порядку, виділена у стандартах **жирним шрифтом**. Стандарти ITAF періодично переглядаються для постійного покращення та внесення змін, які диктуються потребою відповідати на нові виклики у сфері аудиту та підтвердження довіри до ІС.

Положення стандартів

Для полегшення пошуку нижче наведено обов'язкові положення стандартів.

Загальні

1001 Статут аудиту

1001.1 Функція аудиту та підтвердження довіри до ІС повинна бути належним чином задокументованою у статуті аудиту, включаючи цілі, обов'язки, повноваження та підзвітність.

1001.2 Функція аудиту та підтвердження довіри до ІС повинна мати статут аудиту, попередньо узгоджений і затверджений на відповідному рівні організації.

1002 Організаційна незалежність

1002.1 Для забезпечення об'єктивності при виконанні завдань з аудиту та підтвердження довіри функція аудиту та підтвердження довіри до ІС повинна бути незалежною від сфери та виду діяльності, що перевіряються.

1003 Професійна незалежність

1003.1 Фахівці з аудиту та підтвердження довіри до ІС повинні бути незалежними та об'єктивними у своїх ставленнях і проявах у всіх питаннях, які стосуються виконання завдань з аудиту та підтвердження довіри.

1004 Обґрунтовані очікування

1004.1 Фахівці з аудиту та підтвердження довіри до ІС повинні мати обґрунтовані очікування, що аудиторське завдання може бути успішно завершене згідно зі стандартами аудиту та підтвердження довіри до ІС і, за необхідності, іншими відповідними професійними чи галузевими стандартами та діючими нормами, щоб у результаті сформувати своє професійне судження чи аудиторський висновок.

1004.2 Фахівці з аудиту та підтвердження довіри до ІС повинні мати обґрунтовані очікування щодо обсягу робіт завдань з аудиту, який має бути таким, щоб забезпечити можливість дійти до висновку про об'єкт перевірки та вирішити питання, пов'язані з будь-якими обмеженнями.

1004.3 Фахівці з аудиту та підтвердження довіри до ІС повинні мати обґрунтовані очікування щодо усвідомлення керівництвом своїх обов'язків та відповідальності, пов'язаних із своєчасним забезпеченням аудиторів належною та відповідною інформацією, необхідною для виконання поставлених завдань.

1005 Належна професійна ретельність

1005.1 Фахівці з аудиту та підтвердження довіри до ІС повинні проявляти належну професійну ретельність, у тому числі дотримуватись діючих професійних стандартів аудиту при плануванні, виконанні та звітуванні за результатами виконання завдань.

1006 Професійність

1006.1 Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні колективно володіти необхідними навичками і проявляти професійність при виконанні завдань з аудиту та підтвердження довіри до ІС, а також бути професійно компетентними для здійснення роботи.

1006.2 Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні мати достатні знання про об'єкт перевірки.

1006.3 Фахівці з аудиту та підтвердження довіри до ІС повинні підтримувати свою професійну компетентність, постійно отримуючи додаткову професійну освіту та підготовку.

1007 Твердження

1007.1 Фахівці з аудиту та підтвердження довіри до ІС повинні ознайомитися із твердженнями, на відповідність яким здійснюватиметься оцінка об'єкта перевірки, для визначення того, чи такі твердження можна піддати аудиту, і чи є вони достатніми, обґрунтованими та відповідними.

1008 Критерії

1008.1 Фахівці з аудиту та підтвердження довіри до ІС повинні визначити такі критерії, за якими оцінюватиметься об'єкт перевірки, що будуть об'єктивними, повними, відповідними, вимірюваними, зрозумілими, загальновизнаними, достовірними і доступними для всіх читачів чи користувачів звіту.

1008.2 Фахівці з аудиту та підтвердження довіри до ІС повинні вивчати джерела критеріїв аудиту та віддавати перевагу використанню тих критеріїв, які створені відповідними уповноваженими організаціями, порівняно з менш відомими критеріями.

Виконання

1201 Планування завдань

1201.1 Фахівці з аудиту та підтвердження довіри до ІС повинні планувати кожне завдання з аудиту та підтвердження довіри до ІС таким чином, щоб воно відповідало:
- цілі (цілям), обсягу, часовим рамкам і запланованим результатам;
- діючим законам і професійним стандартам аудиту;
- застосуванню ризик-орієнтованого підходу, де це можливо;
- питанням, що виникають у зв'язку зі специфікою завдань;
- вимогам до документації та звітності.

1201.2 Фахівці з аудиту та підтвердження довіри до ІС повинні розробляти та документально оформляти для кожного проекту план завдань з аудиту та підтвердження довіри до ІС, що описує:
- характер, цілі та часові рамки завдань, а також потреби у ресурсах;
- терміни проведення та обсяг аудиторських процедур, необхідних для виконання завдань.

1202 Оцінювання ризиків при плануванні

1202.1 Функція аудиту та підтвердження довіри до ІС повинна застосовувати ризик-орієнтований підхід та відповідну методологію для розроблення загального плану аудиту ІС і визначення пріоритетів для ефективного розподілу ресурсів аудиту ІС.

1202.2 При плануванні індивідуальних завдань фахівці з аудиту та підтвердження довіри до ІС повинні визначати та оцінювати ризики, пов'язані зі сферою, що перевіряється.

1202.3 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики, пов'язані з об'єктом перевірки, ризики аудиту та інші відповідні ризики для організації.

1203 Ефективність і нагляд

1203.1 Фахівці з аудиту та підтвердження довіри до ІС повинні здійснювати роботу у відповідності до затвердженого плану аудиту ІС для того, щоб врахувати виявлені ризики, та в рамках узгодженого графіку.

1203.2 Фахівці з аудиту та підтвердження довіри до ІС повинні забезпечити контроль за роботою персоналу аудиту, яким вони керують, щоб досягти цілей аудиту у відповідності до діючих професійних стандартів аудиту.

1203.3 Фахівці з аудиту та підтвердження довіри до ІС повинні братися за виконання тільки таких задач, які можна завершити за допомогою уже наявних знань і навичок, або якщо вони мають обґрунтовані очікування щодо набуття таких навичок у процесі роботи чи виконання задач під наглядом.

1203.4 Для досягнення цілей аудиту фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази. Результати та висновки аудиту повинні супроводжуватись відповідним аналізом і тлумаченням таких доказів.

1203.5 Фахівці з аудиту та підтвердження довіри до ІС повинні документально оформляти процес аудиту, описуючи аудиторську роботу та аудиторські докази, що обґрунтовують результати та висновки.

1203.6 Фахівці з аудиту та підтвердження довіри до ІС повинні визначати та робити висновки щодо результатів.

1204 Суттєвість

1204.1 При плануванні завдань фахівці з аудиту та підтвердження довіри до ІС повинні враховувати потенційні недоліки або відсутність контролів, а також те, чи можуть призвести до значного порушення чи суттєвого недоліку такі недоліки або відсутність контролів.

1204.2 При визначенні характеру, часових рамок та обсягу процедур аудиту фахівці з аудиту та підтвердження довіри до ІС повинні враховувати суттєвість аудиту та її зв'язок із ризиком аудиту.

1204.3 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати сукупний ефект незначного браку контролів і вразливих місць, а також те, чи може така відсутність контролів створити значне порушення чи суттєвий недолік.

1204.4 У своїх звітах фахівці з аудиту та підтвердження довіри до ІС повинні розкривати наступне:
- відсутність контролів чи їх неефективність;
- значущість порушення контролів;
- ймовірність того, що такі вразливі місця призведуть до значного порушення чи суттєвого недоліку.

1205 Докази

1205.1 Фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази, щоб зробити обґрунтовані висновки, на які спиратимуться результати завдань з аудиту.

1205.2 Фахівці з аудиту та підтвердження довіри до ІС повинні оцінювати достатність отриманих доказів для обґрунтування висновків і досягнення цілей завдань.

1206 Залучення інших експертів

1206.1 Фахівці з аудиту та підтвердження довіри до ІС повинні, за необхідності, розглядати можливість залучення інших експертів для виконання завдань.

1206.2 Фахівці з аудиту та підтвердження довіри до ІС повинні оцінювати та підтверджувати відповідність професійних кваліфікацій, компетенції, належного досвіду, ресурсів, незалежності та процесів контролю якості інших експертів до початку виконання завдань.

1206.3 В рамках виконання своїх завдань фахівці з аудиту та підтвердження довіри до ІС повинні вивчати та оцінювати роботу інших експертів, а також документально оформляти висновки щодо обсягу залучення таких експертів і покладання на результати їх роботи.

1206.4 Фахівці з аудиту та підтвердження довіри до ІС повинні визначати, чи є робота інших експертів, які не є членами групи, що виконує завдання, достатньо адекватною та вичерпною для досягнення поточних цілей завдань, а також чітко документально оформляти свої висновки.

1206.5 Фахівці з аудиту та підтвердження довіри до ІС повинні визначати, чи можна вважати роботу інших експертів надійною і безпосередньо включати її або посилатися на неї у звіті.

1206.6 Фахівці з аудиту та підтвердження довіри до ІС повинні застосовувати додаткові процедури перевірки для отримання достатніх та відповідних доказів, якщо їх не надає робота інших експертів.

1206.7 Фахівці з аудиту та підтвердження довіри до ІС повинні надавати відповідні аудиторські оцінки або висновки та включати в них будь-які обмеження обсягу робіт, якщо необхідні докази не можна отримати за допомогою додаткових процедур перевірки.

1207 Невідповідності та незаконні дії

1207.1 При виконанні завдань фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики існування невідповідностей та незаконних дій.

1207.2 При виконанні завдань фахівці з аудиту та підтвердження довіри до ІС повинні дотримуватись позиції професійного скептицизму.

1207.3 Фахівці з аудиту та підтвердження довіри до ІС повинні документально оформляти та вчасно звітувати перед відповідними особами про будь-які суттєві невідповідності чи незаконні дії.

Звітування

1401 Звітування

1401.1 Фахівці з аудиту та підтвердження довіри до ІС повинні звітувати про результати виконаних завдань, включаючи:

- ідентифікацію організації, очікуваних отримувачів звіту та будь-які обмеження щодо змісту та розповсюдження;
- обсяг, цілі та період виконання завдань, а також характер, визначення терміну проведення та обсягу робіт, що були виконані;
- результати, висновки та рекомендації;
- будь-які кваліфікаційні обмеження фахівців з аудиту та підтвердження довіри до ІС чи обмеження обсягу робіт, що стосуються виконання завдань;
- підпис, дату та розповсюдження згідно з умовами статуту аудиту та контракту.

1401.2 Фахівці з аудиту та підтвердження довіри до ІС повинні гарантувати, що наведені в аудиторському звіті результати ґрунтуються на достатніх та відповідних аудиторських доказах.

1402 Подальша діяльність

1402.1 Фахівці з аудиту та підтвердження довіри до ІС повинні проводити моніторинг відповідної інформації, щоб зробити висновок, чи керівництво своєчасно запланувало / вжило необхідні заходи для розгляду результатів та рекомендацій аудиторського звіту.

Загальні стандарти

Загальні стандарти – це основні принципи, згідно з якими працюють фахівці у галузі підтвердження довіри до ІС. Вони регулюють виконання усіх завдань та описують етику, незалежність, об'єктивність, належну професійну ретельність, знання, компетенцію та навички фахівців з аудиту та підтвердження довіри до ІС.

Виконуючи завдання з аудиту та підтвердження довіри до ІС, фахівці з аудиту та підтвердження довіри до ІС повинні приймати низку ключових рішень стосовно об'єкта перевірки і критеріїв, за якими оцінюється об'єкт перевірки. Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цільові орієнтири, згідно з якими виконуватимуться завдання (стандарти) та за якими оцінюватиметься об'єкт перевірки (критерії).

Загальні стандарти:
1001 Статут аудиту
1002 Організаційна незалежність
1003 Професійна незалежність
1004 Обґрунтовані очікування
1005 Належна професійна ретельність
1006 Професійність
1007 Твердження
1008 Критерії

Усі стандарти описані тут вичерпно. Визначення підкреслених слів наведені у розділі «Терміни». Посилання на окремі стандарти можна отримати на наступній сторінці: www.isaca.org/standard.

1001 Статут аудиту

Положення

1001.1 Функція аудиту та підтвердження довіри до ІС повинна бути належним чином задокументованою у статуті аудиту, включаючи цілі, обов'язки, повноваження та підзвітність.

1001.2 Функція аудиту та підтвердження довіри до ІС повинна мати статут аудиту, попередньо узгоджений і затверджений на відповідному рівні організації.

Ключові аспекти

Функція аудиту та підтвердження довіри до ІС повинна:

- підготувати статут аудиту для визначення обсягу діяльності функції внутрішнього аудиту та підтвердження довіри до ІС на достатньо детальному рівні, щоб звітувати про:
  - повноваження, мету, обов'язки та обмеження функції аудиту та підтвердження довіри до ІС;
  - незалежність і підзвітність функції аудиту та підтвердження довіри до ІС;
  - ролі та обов'язки організації, яка підлягає аудиту, протягом виконання завдань з аудиту ІС або завдань з підтвердження довіри;
  - професійні стандарти, якими керуються фахівці з аудиту та підтвердження довіри до ІС при виконанні завдань з аудиту та підтвердження довіри до ІС;
- переглядати статут аудиту щорічно або й частіше у випадку зміни обов'язків;
- за необхідності, оновлювати статут аудиту, щоб завжди належним чином документувати цілі та обов'язки;
- офіційно надавати організації, яка підлягає аудиту, статут аудиту для кожного завдання з аудиту та підтвердження довіри до ІС.

Терміни

Термін	Визначення
Завдання з аудиту	Конкретне аудиторське завдання, задача або перевірка, як, наприклад, аудит, перевірка контролю, самооцінювання, розслідування фактів шахрайства або надання консультацій. Завдання з аудиту може включати різноманітні задачі або дії, спрямовані на досягнення певної низки пов'язаних цілей.
Завдання з підтвердження довіри	Об'єктивна перевірка доказів з метою надання оцінки процесів управління ризиками, контролю і корпоративного управління в організації. **Примітка до сфери використання документу.** Приклади можуть включати завдання з підтвердження довіри у сфері фінансів, ефективності, відповідності встановленим нормам і безпеки.
Незалежність	Свобода від обставин, що загрожують об'єктивності чи створюють враження об'єктивності. Необхідно, щоб такі загрози об'єктивності нейтралізувалися на рівні окремого аудитора, завдання і на функціональному та організаційному рівнях. Незалежність включає в себе незалежність у поглядах і незалежність у проявах.
Статут аудиту	Документ, затверджений особами, відповідальними за корпоративне управління, що визначає мету, повноваження та відповідальність щодо дій внутрішнього аудиту. Статут повинен: • встановлювати роль внутрішнього аудиту в організації; • санкціонувати доступ до документації, персоналу та майна, необхідних для виконання завдань з аудиту та підтвердження довіри до ІС; • визначати сферу діяльності аудиту.

Зв'язок із настановами

Тип	Назва
Настанова	2001 Статут аудиту

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1002 Організаційна незалежність

Положення

1002.1 Для забезпечення об'єктивності при виконанні завдань з аудиту та підтвердження довіри функція аудиту та підтвердження довіри до ІС повинна бути незалежною від сфери та виду діяльності, що перевіряються.

Ключові аспекти

Функція аудиту та підтвердження довіри до ІС повинна:

- звітувати такому рівню керівництва в організації, що підлягає аудиту, який забезпечує організаційну незалежність і дає можливість функції аудиту та підтвердження довіри до ІС виконувати свої обов'язки без втручання інших осіб;
- розкривати відповідним сторонам деталі про порушення, якщо незалежність є обмеженою або може сприйматися як така;
- уникати виконання неаудиторських ролей в ініціативах, пов'язаних з ІС, що вимагають прийняття на себе керівних обов'язків, оскільки у майбутньому це може обмежувати незалежність;
- описувати незалежність та підзвітність функції аудиту у статуті та / або контракті.

Терміни

Термін	Визначення
Незалежність	Свобода від обставин, що загрожують об'єктивності чи створюють враження об'єктивності. Необхідно, щоб такі загрози об'єктивності нейтралізувалися на рівні окремого аудитора, завдання і на функціональному та організаційному рівнях. Незалежність включає в себе незалежність у поглядах та незалежність у проявах.
Незалежність у поглядах	Стан мислення, що дозволяє робити висновки, не зазнаючи жодних впливів, які можуть скомпрометувати професійні судження, дозволяючи фахівцю діяти цілісно та проявляти об'єктивність і професійний скептицизм.
Незалежність у проявах	Ухиляння від фактів та обставин, які є настільки значущими, що розсудлива інформована третя особа, зваживши усі підтверджуючі конкретні факти та обставини, може дійти до висновку про компрометацію цілісності, об'єктивності чи професійного скептицизму аудиторів або члена аудиторської групи.
Об'єктивність	Здатність неупереджено висловлювати судження, робити висновки та давати рекомендації.
Порушення	Умови, які викликають погіршення або за яких послаблюється здатність досягати цілей аудиту. Порушення організаційної незалежності та індивідуальної об'єктивності може виникати внаслідок особистого конфлікту інтересів, обмеження обсягів, обмеження доступу до документів, персоналу, обладнання чи майна та обмеження ресурсів (таких як фінансування або кадрове забезпечення).

Зв'язок із настановами

Тип	Назва
Настанова	2002 Організаційна незалежність

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1003 Професійна незалежність

Положення

1003.1 Фахівці з аудиту та підтвердження довіри до ІС повинні бути незалежними та об'єктивними у своїх ставленнях і проявах у всіх питаннях, які стосуються виконання завдань з аудиту та підтвердження довіри.

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- при виконанні завдань з аудиту та підтвердження довіри до ІС розглядати проблеми підтвердження довіри та робити висновки справедливо та неупереджено;
- бути незалежними та завжди сприйматися як такі;
- повідомляти відповідні сторони про деталі щодо порушень, якщо незалежність є обмеженою або може сприйматися як така;
- постійно оцінювати незалежність з керівництвом та аудиторським комітетом за умови існування останнього;
- уникати виконання неаудиторських ролей в ініціативах, пов'язаних з ІС, що вимагають прийняття на себе керівних обов'язків, оскільки у майбутньому це може обмежувати незалежність.

Терміни

Термін	Визначення
Незалежність	Свобода від обставин, що загрожують об'єктивності чи створюють враження об'єктивності. Необхідно, щоб такі загрози об'єктивності нейтралізувалися на рівні окремого аудитора, завдання і на функціональному та організаційному рівнях. Незалежність включає в себе незалежність у поглядах і незалежність у проявах.
Незалежність у поглядах	Стан мислення, що дозволяє робити висновки, не зазнаючи жодних впливів, які можуть скомпрометувати професійні судження, дозволяючи фахівцю діяти цілісно та проявляти об'єктивність і професійний скептицизм.
Незалежність у проявах	Ухиляння від фактів та обставин, які є настільки значущими, що розсудлива інформована третя особа, зваживши усі підтверджуючі конкретні факти та обставини, може дійти до висновку про компрометацію цілісності, об'єктивності чи професійного скептицизму аудиторів або члена аудиторської групи.
Об'єктивність	Здатність неупереджено висловлювати судження, робити висновки та давати рекомендації.
Порушення	Умови, які викликають погіршення або за яких послаблюється здатність досягати цілей аудиту. Порушення організаційної незалежності та індивідуальної об'єктивності може виникати внаслідок особистого конфлікту інтересів, обмеження обсягів, обмеження доступу до документів, персоналу, обладнання чи майна та обмеження ресурсів (таких як фінансування або кадрове забезпечення).

Зв'язок із настановами

Тип	Назва
Настанова	2003 Професійна незалежність

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1004 Обґрунтовані очікування

Положення

1004.1 Фахівці з аудиту та підтвердження довіри до ІС повинні мати обґрунтовані очікування щодо виконання завдань згідно зі стандартами аудиту та підтвердження довіри до ІС і, за необхідності, іншими відповідними професійними чи галузевими стандартами та діючими нормами, щоб у результаті висловити свою професійну думку чи висновок.

1004.2 Фахівці з аудиту та підтвердження довіри до ІС повинні мати обґрунтовані очікування щодо обсягу завдань, який має бути таким, щоб забезпечити надання висновку про об'єкт перевірки та вирішити питання, пов'язані з будь-якими обмеженнями.

1004.3 Фахівці з аудиту та підтвердження довіри до ІС повинні мати обґрунтовані очікування щодо усвідомлення керівництвом своїх обов'язків та відповідальності, пов'язаних із своєчасним забезпеченням належною відповідною інформацією, необхідною для виконання поставлених завдань.

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- братися за виконання завдань з аудиту та підтвердження довіри до ІС, тільки якщо можна виконати роботу у відповідності до професійних стандартів;
- братися за виконання завдання з аудиту та підтвердження довіри до ІС, тільки якщо об'єкт перевірки можна оцінювати за відповідними критеріями;
- переглядати обсяг завдань з аудиту та підтвердження довіри до ІС, щоб він був чітко оформлений документально та дозволяв робити висновки щодо об'єкта перевірки;
- розглядати та визначати, чи враховуються всі обмеження, накладені на завдання, включаючи вчасний доступ до належної відповідної інформації;
- враховувати, чи є обсяг достатнім для того, щоб надати аудиторський висновок щодо об'єкта перевірки; обмеження обсягу можуть мати місце, якщо інформація, необхідна для виконання завдань, відсутня, часові рамки для виконання завдань з аудиту та підтвердження довіри до ІС достатньо вузькі, або керівництво намагається обмежити обсяг до обраних сфер; у таких випадках можна розглядати інші типи завдань, такі як обґрунтування фінансових положень, що підлягають аудиту, перегляд контролів, відповідність необхідним стандартам і практикам або відповідність договорам, ліцензіям, законодавчим і нормативним актам.

Терміни

Термін	Визначення
Аудиторський висновок	Офіційний висновок фахівця з аудиту та підтвердження довіри до ІС, що описує обсяг аудиту, процедури, які застосовувалися для підготовки звіту, а також те, чи підтверджують результати відповідність критеріям аудиту. Існують наступні типи висновків: • **безумовний висновок** (не встановлено жодних порушень, або жодне із встановлених порушень не призводить у сукупності до значного порушення); • **обмежений висновок** (вказує на порушення, які у сукупності призводять до значного порушення, але яке не є суттєвим недоліком); • **негативний висновок** (встановлює одне чи кілька значних порушень, які у сукупності призводять до суттєвого недоліку). **Примітка.** Відмова від аудиторського висновку надається, коли аудитор не може отримати відповідні аудиторські докази в обсязі, достатньому для формування на них свого висновку, або якщо неможливо сформувати такий висновок у зв'язку з потенційними взаємодіями різних невизначеностей та їх можливого сукупного впливу.

Зв'язок із настановами

Тип	Назва
Настанова	2004 Обґрунтовані очікування

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1005 Належна професійна ретельність

Положення

1005.1 Фахівці з аудиту та підтвердження довіри до ІС повинні проявляти належну професійну ретельність, у тому числі дотримуватись діючих професійних стандартів аудиту при плануванні, виконанні та звітуванні за результатами завдань.

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- виконувати завдання цілісно та ретельно;
- демонструвати розуміння та компетенцію в обсязі, достатньому для досягнення цілей завдань;
- при виконанні завдань дотримуватися позиції професійного скептицизму;
- підтримувати професійну компетентність, постійно ознайомлюючись із нововведеннями у сфері професійних стандартів та дотримуючись їх виконання;
- при проведенні завдань обговорювати з членами групи їх ролі та обов'язки і забезпечувати дотримання групою відповідних стандартів;
- при проведенні завдань розглядати всі ускладнення у відповідності до стандартів, що застосовуються;
- при виконанні завдань ефективно взаємодіяти з відповідними зацікавленими сторонами;
- вживати всі необхідні заходи для захисту інформації, отриманої або встановленої під час виконання завдань, від випадкового розголошення або розкриття неуповноваженим особам;
- проводити всі завдання, проявляючи достатню впевненість у поглядах; рівень тестування залежатиме від типу завдань.

Примітка. Належна професійна ретельність передбачає достатню ретельність і компетентність, а не непогрішимість або екстраординарну діяльність аудитора.

Терміни

Термін	Визначення
Професійний скептицизм	Ставлення, яке включає допитливе мислення та критичну оцінку аудиторських доказів. Джерело: AU 230.07, AICPA.

Зв'язок із настановами

Тип	Назва
Настанова	2005 Належна професійна ретельність

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1006 Професійність

Положення

1006.1 Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні колективно володіти необхідними навичками і проявляти професійність при виконанні завдань з аудиту та підтвердження довіри до ІС, а також бути професійно компетентними для здійснення роботи.

1006.2 Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні мати достатні знання про об'єкт перевірки.

1006.3 Фахівці з аудиту та підтвердження довіри до ІС повинні підтримувати свою професійну компетентність, здобуваючи додаткову професійну освіту та підготовку.

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- демонструвати належний рівень професійної компетентності (навичок, знань і досвіду, необхідних для виконання запланованих завдань) до початку роботи;
- оцінювати альтернативні способи отримання необхідних навичок, включаючи залучення підрядників або третіх осіб до виконання частини задач, відстрочування виконання завдань до отримання необхідних навичок, або забезпечення наявності необхідних навичок іншим способом;
- переконатись, що члени групи, залучені до виконання завдань з аудиту та підтвердження довіри до ІС, які не є власниками сертифікату CISA і не мають жодних інших відповідних офіційних професійних звань, мають достатній освітній рівень, підготовку та досвід роботи;
- при управлінні групою під час проведення завдань з аудиту та підтвердження довіри до ІС забезпечувати достатню впевненість у тому, що всі члени групи мають відповідну професійну компетентність для роботи, яку вони виконують;
- мати достатні знання про ключові сфери діяльності для раціонального та ефективного виконання завдань з аудиту та підтвердження довіри до ІС, як і інші залучені фахівці та члени групи;
- дотримуватись вимог, які ставляться перед власниками сертифікату CISA або інших відповідних професійних звань, щодо додаткової професійної освіти та розвитку;
- постійно вдосконалювати свої професійні знання, відвідуючи освітні курси, семінари, конференції, онлайн-конференції та курси за місцем роботи для надання професійних послуг на такому рівні, який відповідає вимогам ролі фахівця з аудиту та підтвердження довіри до ІС.

Терміни

Термін	Визначення
Компетенція	Здатність успішно виконувати конкретну задачу, дію або функцію.
Професійність	Володіння навичками та досвідом.

Зв'язок із настановами

Тип	Назва
Настанова	2006 Професійність

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1007 Твердження

Положення

1007.1 Фахівці з аудиту та підтвердження довіри до ІС повинні перевіряти твердження, на основі яких здійснюватиметься оцінка об'єкта перевірки, для визначення того, чи такі твердження можна піддати аудиту, і чи є вони достатніми, обґрунтованими та відповідними.

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- визначати критерії, за якими здійснюватиметься оцінка об'єкта перевірки, для підтвердження того, що вони підтримують твердження;
- визначати, чи такі твердження можуть бути перевірені під час аудиту, і чи обґрунтовуються вони підтверджуючою інформацією;
- визначати, чи такі твердження ґрунтуються на належним чином встановлених критеріях, які піддаються об'єктивному аналізу та виміру;
- якщо твердження розроблені керівництвом, переконатись, що при їх порівнянні з іншими офіційно виданими стандартами такі твердження будуть достатніми для обізнаного читача чи користувача;
- якщо твердження розроблені третіми особами, які здійснюють контролі від імені організації, переконатись, що керівництво перевірило та прийняло такі твердження;
- звітувати безпосередньо щодо об'єкта перевірки (пряме звітування) або щодо тверджень про об'єкт перевірки (непряме звітування);
- робити висновок про кожне твердження, ґрунтуючись на сукупних даних щодо критеріїв і на власних професійних судженнях.

Терміни

Термін	Визначення
Твердження	Будь-яке офіційне висловлювання чи ряд висловлювань керівництва про об'єкт перевірки. Як правило, твердження надаються у письмовій формі та містять список певних характеристик конкретного об'єкта перевірки або процесу, у який його залучено

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1008 Критерії

Положення

1008.1 Фахівці з аудиту та підтвердження довіри до ІС повинні визначити такі критерії, за якими оцінюватиметься об'єкт перевірки, що будуть об'єктивними, повними, відповідними, вимірними, зрозумілими, загальновизнаними, достовірними і доступними для всіх читачів чи користувачів звіту.

1008.2 Фахівці з аудиту та підтвердження довіри до ІС повинні розглядати джерело критеріїв і зосереджуватись на виданих відповідними повноважними органами до прийняття менш відомих критеріїв.

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- ретельно підходити до вибору критеріїв і бути в змозі підтвердити свій вибір;
- застосовувати свої професійні судження для підтвердження того, що у випадку використання критеріїв, з їх допомогою буде надано справедливу та об'єктивну професійну думку чи висновок, який не буде дезінформувати читачів чи користувачів; допускається, що керівництво може задати такі критерії, які не відповідатимуть усім вимогам;
- при визначенні вимог до завдань враховувати придатність і доступність критеріїв;
- якщо критерії є важкодоступними, неповними чи потребують пояснень, надавати опис або будь-яку іншу інформацію, необхідну для того, щоб звіт був справедливим, об'єктивним і зрозумілим, а також описував контекст, у якому застосовуються критерії.

Придатність і доречність критеріїв оцінки об'єкта перевірки повинні визначатися за наступними п'ятьма критеріями придатності:

- **об'єктивність** (критерії повинні бути неупередженими, щоб не впливати на результати та висновки фахівців і, відповідно, не дезінформувати користувачів звіту);
- **повнота** (критерії повинні бути повними, щоб при виконанні завдання з аудиту та підтвердження довіри до ІС визначати і застосовувати усі критерії, які можуть впливати на висновки фахівців про об'єкт перевірки);
- **відповідність** (критерії повинні відповідати об'єкту перевірки і сприяти отриманню результатів та висновків, що відповідають цілям завдання з аудиту та підтвердження довіри до ІС);
- **вимірність** (у випадку застосування критеріїв різними фахівцями за таких самих умов вони повинні однаково вимірювати об'єкт перевірки і робити однакові висновки);
- **зрозумілість** (критерії повинні бути чіткими і не мати значних відмінностей при їх тлумаченні цільовими користувачами).

На прийнятність критеріїв впливає їх доступність для користувачів звітів. Таким чином, користувачі повинні розуміти основи діяльності з підтвердження довіри і відповідність результатів та висновків фахівців. Джерела можуть містити критерії, які є:

- **загальновизнаними** (критерії повинні бути загальновизнаними, щоб цільові користувачі не ставили під сумнів їхнє застосування);
- **достовірними** (критерії повинні бути обрані таким чином, щоб відображати офіційні положення у своїй сфері і підходити для об'єкта перевірки; наприклад, офіційні положення можуть бути видані професійними організаціями, галузевими групами, урядовими або регуляторними органами);
- **загальнодоступними** (критерії повинні бути доступними для користувачів звітів; наприклад, стандарти, розроблені професійними бухгалтерськими та аудиторськими органами, такими як ISACA, IFAC[10] та іншими загальновизнаними урядовими чи професійними органами);
- **доступними для всіх користувачів** (якщо критерії не є загальнодоступними, їх необхідно описати для всіх користувачів у розділі «Твердження», який є частиною звіту. Твердження складаються з положень про об'єкт перевірки, які відповідають вимогам «придатних критеріїв» і можуть бути перевіреними).

При виборі критеріїв підтвердження довіри до ІС, окрім придатності та доступності, необхідно також розглядати їх джерело, враховуючи їх застосування та потенційну аудиторію. Наприклад, у випадку державного регулювання найбільш прийнятно обрати критерії, що ґрунтуються на твердженнях щодо об'єкта перевірки, розроблених законодавчими чи регуляторними органами. В іншому випадку прийнятними будуть критерії галузевих чи торгових асоціацій. Нижче наведено можливі джерела критеріїв у порядку їх розгляду.

- **Критерії, встановлені ISACA,** – це загальнодоступні критерії та стандарти, які пройшли

[10] IFAC (International Federation of Accountants) – Міжнародна федерація бухгалтерів

1008 Критерії (продовження)

Ключові аспекти (продовження)

рецензування і ретельний процес комплексної перевірки загальновизнаними міжнародними експертами у сфері корпоративного управління, контролю, безпеки та підтвердження довіри IT.

- **Критерії, встановлені іншими експертними органами,** схожі на стандарти та критерії ISACA; вони відповідають об'єкту перевірки і були розроблені та пройшли рецензування і ретельний процес комплексної перевірки експертами у різних сферах.
- **Критерії, встановлені законодавчими чи регуляторними органами,** необхідно застосовувати з обережністю, оскільки закони та нормативні документи можуть бути основою критеріїв; формулювання часто є комплексними і несуть специфічне юридичне значення; у багатьох випадках необхідно формулювати вимоги як твердження; у подальшому свою професійну думку щодо законів, як правило, виражають виключно фахівці у сфері юриспруденції.
- **Критерії, встановлені організаціями без дотримання процесуальних норм,** включають в себе відповідні критерії, розроблені іншими організаціями без дотримання процесуальних норм, загальних обговорень і дискусій.
- **Критерії, розроблені виключно для виконання завдань з аудиту та підтвердження довіри до ІС,** необхідно застосовувати з особливою обережністю, щоб вони відповідали критеріям придатності, зокрема, повноти, можливості оцінювання та об'єктивності. Критерії, розроблені виключно для виконання завдань з аудиту та підтвердження довіри до ІС, подаються у формі тверджень.

Необхідно ретельно підходити до вибору критеріїв. Оскільки важливо дотримуватися місцевих законів та нормативних документів, і це повинно бути обов'язковою вимогою, вважається, що багато завдань з аудиту та підтвердження довіри до ІС охоплюють такі сфери, як управління змінами, загальні контролі IT та контролі доступу, що не охоплюються законами та нормативними документами. Окрім того, деякі галузі, як, наприклад, галузь платіжних карток, встановили обов'язкові вимоги, яких необхідно дотримуватись. Якщо законодавчі вимоги є основоположним принципом, фахівці повинні забезпечити відповідність обраних критеріїв цілям завдань.

У рамках виконання завдань додаткова інформація може показати, що певні критерії не потрібні для досягнення цілей. За таких умов відпадає потреба у подальшій роботі над ними.

Терміни

Термін	Визначення
Критерії	Стандарти та показники, що застосовуються для вимірювання та представлення об'єкта перевірки, відповідно до яких аудитор ІС оцінює об'єкт перевірки. Критерії повинні бути: • об'єктивними (неупередженими); • повними (такими, що містять усі відповідні фактори для того, щоб зробити висновок); • відповідними(такими, що відносяться до об'єкта перевірки); • вимірними (такими, що передбачають постійне вимірювання); • зрозумілими. В атестаційних завданнях можуть оцінюватися показники, які були визначені керівництвом як письмові твердження щодо об'єкта перевірки. Практикуючий фахівець готує свій висновок щодо об'єкта перевірки, виходячи з відповідних критеріїв.

Зв'язок із настановами

Тип	Назва
Настанова	2008 Критерії

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

Стандарти виконання

Стандарти виконання описують основні очікування щодо проведення завдань з аудиту та підтвердження довіри до ІС. Оскільки ці стандарти застосовуються до фахівців з аудиту та підтвердження довіри до ІС, які виконують будь-які завдання з аудиту та підтвердження довіри до ІС, особливо важливо дотримуватися їх в аудиторській діяльності. Таким чином, стандарти виконання звертають увагу фахівців з аудиту та підтвердження довіри до ІС на опис і проведення роботи з підтвердження довіри, необхідні докази та надання результатів і висновків щодо аудиту та підтвердження довіри до ІС.

Стандарти виконання:
1201 Планування завдань
1202 Оцінювання ризиків у плануванні
1203 Ефективність і нагляд
1204 Суттєвість
1205 Докази
1206 Залучення інших експертів
1207 Невідповідності та незаконні дії

Усі стандарти описані тут вичерпно. Визначення підкреслених слів наведені у розділі «Терміни». Посилання на окремі стандарти можна отримати на наступній сторінці: www.isaca.org/standard.

1201 Планування завдань

Положення

1201.1 Фахівці з аудиту та підтвердження довіри до ІС повинні планувати кожне завдання з аудиту та підтвердження довіри до ІС таким чином, щоб воно відповідало:

- **цілі (цілям), обсягу, часовим рамкам і запланованим результатам;**
- **діючим законам і професійним стандартам аудиту;**
- **застосуванню ризик-орієнтованого підходу, де це можливо;**
- **питанням, що виникають у зв'язку зі специфікою завдань;**
- **вимогам до документації та звітності.**

1201.2 Фахівці з аудиту та підтвердження довіри до ІС повинні розробляти та документально оформляти для кожного проекту план завдань з аудиту та підтвердження довіри до ІС, що описує:

- **характер, цілі та часові рамки завдань, а також потреби у ресурсах;**
- **терміни проведення та обсяг аудиторських процедур, необхідних для виконання завдань.**

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- розуміти вид діяльності, який підлягає аудиту; обсяг необхідних знань повинен визначатися у відповідності до характеру організації, її середовища, сфер ризику та цілей завдань;
- розглядати настанови та вказівки щодо об'єкта перевірки в рамках законодавчих і нормативних актів, правил, вказівок і настанов, виданих урядовими органами чи галузевими групами;
- проводити оцінку ризиків для забезпечення достатньої впевненості у тому, що під час виконання завдань будуть охоплені всі важливі складові; після того можуть бути встановлені стратегії аудиту, рівні суттєвості та потреби у ресурсах;
- за допомогою відповідних методик управління проектом розробити проектний план завдань, щоб забезпечити виконання діяльності згідно з графіком і в рамках бюджету;
- включати у план питання, що виникають у зв'язку зі специфікою завдань, як, наприклад:
  - наявність ресурсів та необхідних знань, навичок і досвіду;
  - визначення інструментів, необхідних для збору доказів, проведення тестувань і підготовку / підсумовування інформації для формування звітності;
  - критерії оцінювання, які будуть застосовуватися;
  - вимоги до звітування та розповсюдження;
- документально оформляти проектний план завдань з аудиту та підтвердження довіри до ІС для чіткого визначення:
  - цілі (цілей), обсягу, термінів виконання завдань;
  - ресурсів;
  - ролей та обов'язків;
  - виявлених сфер ризику та їх впливу на план завдань;
  - інструментів та технік, що будуть застосовуватися;
  - майбутніх опитувань для встановлення фактів;
  - відповідної інформації, що буде отримана;
  - процедур перевірки та підтвердження отриманої інформації та її використання як доказів;
  - припущень стосовно підходів, методик, процедур та очікуваних результатів і висновків;
- встановлювати графіки виконання завдань, максимально враховуючи терміни проведення завдань, доступність та інші зобов'язання і вимоги керівництва та організації, яка підлягає аудиту;
- під час виконання завдань з аудиту та підтвердження довіри до ІС коригувати проектний план відповідно до виникаючих ситуацій, таких як нові ризики, неправильні припущення чи результати здійснених процедур;
- виконуючи внутрішні завдання:
  - надавати організації, яка підлягає аудиту, статут аудиту; за необхідності, застосовувати контракт чи його аналог для подальшого уточнення чи підтвердження участі у виконанні окремих завдань;
  - надавати організації, яка підлягає аудиту, план, щоб вона була повною мірою проінформована і мала змогу, за необхідності, забезпечувати доступ до осіб, документації та інших ресурсів;

1201 Планування завдань (продовження)

Ключові аспекти (продовження)

- виконуючи зовнішні завдання:
  – готувати окремі контракти для кожного зовнішнього завдання з аудиту та підтвердження довіри до ІС;
  – готувати проектний план для кожного зовнішнього завдання з аудиту та підтвердження довіри до ІС; такий план повинен, щонайменше, документально оформляти ціль (цілі) та обсяг завдань.

Зв'язок із настановами

Тип	Назва
Настанова	2201 Планування завдань

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1202 Оцінювання ризиків у плануванні

Положення

1202.1 Функція аудиту та підтвердження довіри до ІС повинна застосовувати необхідний підхід до оцінювання ризиків та відповідну допоміжну методику для розроблення загального плану аудиту ІС і визначення пріоритетів для ефективного розподілу ресурсів аудиту ІС.

1202.2 При плануванні індивідуальних завдань фахівці з аудиту та підтвердження довіри до ІС повинні визначати та оцінювати ризики, пов'язані зі сферою, що перевіряється.

1202.3 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики, пов'язані з об'єктом перевірки, ризики аудиту та інші відповідні ризики для організації.

Ключові аспекти

При плануванні поточної діяльності функція аудиту та підтвердження довіри до ІС повинна:

- щорічно проводити та документально оформляти оцінювання ризиків для розробки плану аудиту ІС;
- включати в оцінку ризиків стратегічні плани та цілі організації, а також її структуру управління ризиками та ініціативи;
- для кожного завдання з аудиту та підтвердження довіри до ІС визначати та підтверджувати кількість ресурсів, необхідних для проведення аудиту ІС, щоб відповідати вимогам завдань;
- розробляючи та виконуючи певні завдання з аудиту та підтвердження довіри до ІС, оцінювати ризики при виборі сфер і складових, необхідних для проведення аудиту, а також при прийнятті рішень;
- надавати оцінку ризиків на затвердження зацікавленим та іншим відповідним сторонам;
- на основі оцінки ризиків визначати пріоритети та встановлювати графік роботи з аудиту та підтвердження довіри до ІС;
- на основі оцінки ризиків розробляти план, що:
  - буде основою для діяльності у сфері аудиту та підтвердження довіри до ІС;
  - розглядатиме вимоги та діяльність, не пов'язані з аудитом та підтвердженням довіри до ІС;
  - щорічно переглядатиметься та затверджуватиметься особами, відповідальними за корпоративне управління;
  - описуватиме обов'язки, встановлені у статуті аудиту.

При плануванні індивідуальних завдань фахівці з аудиту та підтвердження довіри до ІС повинні:

- визначати та оцінювати ризики, пов'язані з об'єктом перевірки;
- проводити попередню оцінку ризиків, пов'язаних з об'єктом перевірки, для кожного завдання; цілі кожного окремого завдання повинні відображати результати цієї попередньої оцінки ризиків;
- при розгляді сфер ризику та плануванні окремого завдання враховувати результати попередніх аудитів, перевірки та результати, у тому числі усі коригуючи заходи; окрім того, враховувати загальний процес оцінки ризиків радою директорів підприємства;
- при плануванні та проведенні аудиту ІС намагатися зменшити ризики аудиту до прийнятного рівня та відповідати аудиторським цілям шляхом належної оцінки об'єкта перевірки ІС і пов'язаних контролів;
- при плануванні окремої процедури з аудиту ІС усвідомлювати, що чим нижчий поріг суттєвості, тим точніші аудиторські очікування та більші ризики аудиту;
- для забезпечення додаткової впевненості зменшувати ризики та підвищувати поріг суттєвості шляхом розширення тестування контролів (зменшення ризиків системи контролю) та / або розширення процедур перевірки на суттєвість (зменшення ризиків невиявлення помилок).

Терміни

Термін	Визначення
Оцінювання ризиків	Процес визначення та оцінки ризиків та їх потенційного впливу. Оцінювання ризиків здійснюється для визначення складових або сфер, які представляють найбільший ризик, уразливість або вплив на організацію, для включення до щорічного плану аудиту ІС. Оцінка ризиків також використовується для управління ризиками, пов'язаними зі здійсненням проекту та його вигодами.
Перевірка на суттєвість	Отримання аудиторських доказів щодо повноти, точності чи існування діяльності або операцій у період аудиту.

1202 Оцінювання ризиків у плануванні (продовження)

Терміни (продовження)

Термін	Визначення
Притаманний ризик	Рівень ризику без урахування заходів, які вжило або може вжити керівництво (наприклад, застосування контролів). Дивіться визначення терміну «ризик системи контролю».
Ризик аудиту	Ризик дійти до хибного висновку, ґрунтуючись на результатах аудиту. Є три складових ризику аудиту: • ризик системи контролю; • ризик невиявлення помилок; • ризик, притаманний організації.
Ризик невиявлення помилок	Ризик невиявлення процедурами, які використовують фахівці з аудиту та підтвердження довіри до ІС, помилки, яка може бути значною особисто або у поєднанні з іншими помилками. Дивіться визначення терміну «ризик аудиту».
Ризик, пов'язаний з об'єктом перевірки	Ризик, що відноситься до сфери, яка перевіряється: • бізнес-ризик (платоспроможність клієнта, кредитоспроможність, ринкові фактори тощо); • контрактний ризик (відповідальність, ціни, тип, штрафи тощо); • ризик, притаманний країні (політичний, навколишнє середовище, безпека тощо); • проектний ризик (ресурси, набір навичок, методики, стабільність продукту тощо); • технологічний ризик (рішення, архітектура, система інфраструктури технічного та програмного забезпечення, канали доставки тощо); Дивіться визначення терміну «ризик, притаманний організації».
Ризик системи контролю	Ризик існування значної помилки, яку система внутрішнього контролю не може вчасно виявити або попередити. Дивіться визначення терміну «ризик, притаманний організації».
Статут аудиту	Документ, затверджений особами, відповідальними за корпоративне управління, що визначає мету, повноваження та відповідальність щодо дій внутрішнього аудиту. Статут повинен: • встановлювати роль внутрішнього аудиту в організації; • санкціонувати доступ до документації, персоналу та майна, необхідних для виконання завдань з аудиту ІС і підтвердження довіри до ІС; • визначати сферу діяльності аудиту.
Суттєвість	Аудиторська концепція важливості елемента інформації, враховуючи її вплив чи наслідки на функціонування об'єкта перевірки в цілому. Вираження відносної значущості чи важливості окремого питання в контексті організації в цілому.

Зв'язок із настановами

Тип	Назва
Настанова	2202 Оцінювання ризиків у плануванні

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1203 Ефективність і нагляд

Положення

1203.1 Фахівці з аудиту та підтвердження довіри до ІС повинні здійснювати роботу у відповідності до затвердженого плану аудиту ІС для того, щоб охопити виявлені ризики, та в рамках узгоджених процедур.

1203.2 Фахівці з аудиту та підтвердження довіри до ІС повинні забезпечити контроль за роботою персоналу аудиту, який вони курують, щоб досягти цілей аудиту у відповідності до діючих професійних стандартів аудиту.

1203.3 Фахівці з аудиту та підтвердження довіри до ІС повинні братися за виконання тільки таких задач, які можна завершити за допомогою уже наявних знань і навичок, або якщо вони мають обґрунтовані очікування щодо набуття таких навичок у процесі роботи чи виконання задач під наглядом.

1203.4 Для досягнення цілей аудиту фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази. Результати та висновки аудиту повинні супроводжуватись відповідним аналізом і тлумаченням таких доказів.

1203.5 Фахівці з аудиту та підтвердження довіри до ІС повинні документально оформляти процес аудиту, описуючи аудиторську роботу та аудиторські докази, що обґрунтовують результати та висновки.

1203.6 Фахівці з аудиту та підтвердження довіри до ІС повинні визначати та робити висновки щодо результатів.

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- доручати завдання членам групи, навички та досвід яких відповідає потребам завдань;
- за необхідності, залучати зовнішні ресурси до роботи групи, що займається аудитом ІС, і забезпечувати належний контроль за здійсненням роботи;
- під час виконання завдань управляти ролями та обов'язками окремих членів групи, що проводить аудит ІС, визначаючи, щонайменше:
  - ролі виконавців і перевіряючих;
  - обов'язок щодо розробки методик і підходів;
  - створення програм аудиту та підтвердження довіри;
  - проведення роботи;
  - вирішення гострих ситуацій, ускладнень і проблем у процесі їх виникнення;
  - документальне оформлення та роз'яснення результатів;
  - написання звітів;
- забезпечувати перевірку кожної задачі, виконаної членом (членами) групи, іншим відповідним членом групи;
- застосовувати найкращі доступні аудиторські докази у відповідності до важливості аудиторських цілей, а також часу та зусиль, витрачених на отримання доказів;
- отримувати додаткові докази, якщо згідно із професійним судженням фахівця отримані докази не відповідають критеріям достатності та відповідності для формування професійної думки або підтвердження результатів і висновків;
- організовувати та документально оформляти роботу, що здійснюється під час виконання завдань, дотримуючись попередньо визначених, документально оформлених і затверджених процедур;
- документально оформляти:
  - цілі аудиту та обсяг роботи, програму аудиту, кроки, зроблені під час аудиту, зібрані докази, результати, висновки та рекомендації;
  - деталі, достатні для того, щоб розсудлива інформована особа могла знову виконати задачі, що мали місце під час здійснення роботи, та дійти тих самих висновків;
  - хто виконав кожну задачу, а також роль цієї особи у підготовці та перевірці документації;
  - дати підготовки та перевірки документації;
- отримувати від організації, що підлягає аудиту, відповідні письмові звернення, які чітко деталізують важливі сфери завдань, питання, що виникали, та їх вирішення, а також твердження, зроблені організацією, що підлягає аудиту;
- визначити, чи організація, що підлягає аудиту, підписала та продатувала свої звернення, щоб підтвердити прийняття обов'язків щодо завдань;
- документально оформляти та зберігати у робочій документації всі отримані під час проведення завдань звернення, як письмові, так і усні.

1203 Ефективність і нагляд (продовження)

Зв'язок зі стандартами і настановами

Тип	Назва	
Стандарт	1005	Належна професійна ретельність
Стандарт	1205	Докази
Стандарт	1401	Звітування
Настанова	2202	Оцінювання ризиків у плануванні

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1204 Суттєвість

Положення

1204.1 При плануванні завдань фахівці з аудиту та підтвердження довіри до ІС повинні враховувати потенційні вразливі місця та відсутність контролів, а також те, чи можуть призвести до значного порушення чи суттєвого недоліку такі вразливі місця та відсутність контролів.

1204.2 При визначенні характеру, часових рамок та обсягу процедур аудиту фахівці з аудиту та підтвердження довіри до ІС повинні враховувати суттєвість аудиту та її зв'язок із ризиками аудиту.

1204.3 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати сукупний ефект незначного браку контролів і вразливих місць, а також те, чи така відсутність контролів може перерости у значне порушення чи суттєвий недолік.

1204.4 У своїх звітах фахівців з аудиту та підтвердження довіри до ІС повинні розкривати наступне:

- **відсутність контролів чи їх неефективність;**
- **значущість проблеми порушення контролів;**
- **ймовірність того, що такі вразливі місця призведуть до значного порушення чи суттєвого недоліку.**

Ключові аспекти

При виконанні завдань фахівці з аудиту та підтвердження довіри до ІС повинні:

- застосовувати концепцію суттєвості при:
  – плануванні та виконанні завдань;
  – оцінці впливу окремих складових, процесів або помилок;

Будь-яке порушення, недолік чи брак відповідних політик, процедур і контролів необхідно розглядати в рамках конкретних ситуацій, що виникають під час виконання завдань;

- враховувати визначення суттєвості, надане законодавчими чи регуляторними органами;
- враховувати те, що оцінка суттєвості та ризиків аудиту час від часу може відрізнятися залежно від обставин та зміни середовища;
- при плануванні та виконанні завдання намагатися зменшити ризики аудиту до прийнятного рівня та досягнути його цілей;
- враховувати суттєвість при визначенні характеру, часових рамок та обсягу аудиторських процедур;
- зменшувати ризики аудиту для підвищення порогу суттєвості предметних сфер шляхом розширення тестування контролів (зменшення ризиків системи контролю) та / або розширення процедур перевірки на суттєвість (зменшення ризиків невиявлення помилок);
- оцінювати вплив компенсуючих контролів та їх ефективність при визначенні того, чи проблема порушення контролів або поєднання таких проблем є суттєвим недоліком;
- при визначенні суттєвості враховувати сукупний ефект різних помилок і недоліків контролів;
- враховувати не тільки розмір, а й характер проблем порушення контролів, а також обставини їх виникнення, оцінюючи їх загальний вплив на професійну думку чи висновки фахівця.

Терміни

Термін	Визначення
Ризик аудиту	Ризик дійти до хибного висновку ґрунтуючись на результатах аудиту. Є три складових ризику аудиту: • ризик системи контролю; • ризик невиявлення помилок; • ризик, притаманний організації.
Суттєвий недолік	Порушення чи поєднання порушень внутрішнього контролю, за яких існує значна ймовірність, що суттєва недостовірність не буде вчасно попереджена чи виявлена. Недолік контролю вважається суттєвим, якщо відсутність контролів призводить до неможливості забезпечити достатню довіру до об'єкта контролю, якій він має відповідати. Недолік, який класифікується як суттєвий, означає: • відсутність контролів та / або їх невикористання та / або неадекватність; • гарантоване погіршення. Існує зворотній зв'язок між суттєвістю та рівнем ризиків аудиту, прийнятних для фахівця з аудиту та підтвердження довіри до ІС, тобто чим вищий рівень суттєвості, тим нижча вірогідність виникнення ризиків аудиту, і навпаки.

1204 Суттєвість (продовження)

Терміни (продовження)

Термін	Визначення
Суттєвість	Аудиторська концепція важливості елемента інформації, враховуючи її вплив чи наслідки на функціонування об'єкта перевірки в цілому. Вираження відносної значущості чи важливості окремого питання в контексті організації в цілому.

Зв'язок зі стандартами і настановами

Тип	Назва	
Стандарт	1201	Планування завдань
Стандарт	1202	Оцінювання ризиків у плануванні
Стандарт	1207	Невідповідності та незаконні дії
Стандарт	1401	Звітування
Настанова	2202	Оцінювання ризиків у плануванні
Настанова	2204	Суттєвість

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1205 Докази

Положення

1205.1 Фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази, щоб зробити обґрунтовані висновки, на які спиратимуться результати завдань.

1205.2 Фахівці з аудиту та підтвердження довіри до ІС повинні оцінювати достатність отриманих доказів для обґрунтування висновків і досягнення цілей завдань.

Ключові аспекти

Виконуючи завдання, фахівці з аудиту та підтвердження довіри до ІС повинні:

- отримати достатні та відповідні докази, у тому числі вказати:
  – виконані процедури;
  – результати виконаних процедур;
  – вихідну документацію (в електронному чи паперовому форматі), записи та підтверджуючу інформацію для обґрунтування завдань;
  – висновки та результати завдань;
  – документацію про виконання роботи у відповідності до діючих законів, нормативних документів і політик;
- підготувати документацію, яка повинна:
  – зберігатися і бути доступною у період та у форматі, що відповідає політиці організації щодо аудиту та підтвердження довіри, а також відповідним професійним стандартам, законам і нормативним документам;
  – бути захищеною від несанкціонованого розкриття та зміни протягом її підготовки та зберігання;
  – бути знищеною належним чином після завершення періоду її зберігання;
- при отриманні доказів після перевірки контролів враховувати їх достатність для обґрунтування оціненого рівня ризиків системи контролю;
- належним чином визначати, зіставляти та каталогізувати докази;
- при оцінці надійності доказів враховувати їхні властивості, такі як джерело, характер (наприклад, письмові, усні, візуальні, електронні) та автентичність (наприклад, електронні та власноручні підписи, печатки);
- розглядати найбільш економічно ефективні засоби збору необхідних доказів з мінімальними затратами часу, щоб відповідати цілям і ризикам, пов'язаним із завданнями; однак, ні ускладнення, ні ціна не повинні бути причиною нехтування необхідними процедурами;
- вибирати найбільш відповідні процедури збору доказів в залежності від об'єкта перевірки (тобто його характеру, часових рамок для проведення аудиту, професійних суджень); процедури, які використовують для отримання доказів:
  – опитування та підтвердження;
  – повторне проведення;
  – перерахунки;
  – підрахунки;
  – аналітичні процедури;
  – перевірки;
  – спостереження;
  – інші загальноприйняті методи;
- розглядати джерело та характер будь-якої отриманої інформації для оцінки її надійності та виконання вимог до її подальшого підтвердження; загалом, надійність доказів більша, якщо вони:
  – надані у письмовій, а не усній формі;
  – отримані з незалежних джерел;
  – отримані фахівцями, а не організацією, що підлягає аудиту;
  – засвідчені незалежною стороною;
  – зберігаються незалежною стороною;
  – є результатом перевірки;
  – є результатом спостережень;
- отримувати об'єктивні докази, достатні для того, щоб кваліфікована незалежна сторона могла знову здійснити перевірку та дійти тих самих результатів і висновків;
- отримувати докази, що відповідають суттєвості знахідки, а також наявним ризикам;
- звертати належну увагу на точність і повноту інформації, якщо фахівець з аудиту та підтвердження довіри до ІС отримав її від організації для виконання аудиторських процедур;

1205 Докази (продовження)

Ключові аспекти (продовження)

- розкривати інформацію про будь-які ситуації, в яких неможливо отримати достатні докази у спосіб, що відповідає звітуванню результатів завдань з аудиту та підтвердження довіри до ІС;
- гарантувати безпеку доказів від несанкціонованого доступу та змін;
- після завершення роботи з аудиту та підтвердження довіри до ІС зберігати докази згідно з усіма діючими законами, нормативними документами та політиками.

Терміни

Термін	Визначення
Відповідні докази	Міра якості доказів.
Достатні докази	Міра кількості доказів; обґрунтовують усі суттєві питання щодо цілей та обсягу аудиту. Дивіться визначення терміну «докази».

Зв'язок із настановами

Тип	Назва
Настанова	2205 Докази

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1206 Залучення інших експертів

Положення

1206.1 Фахівці з аудиту та підтвердження довіри до ІС повинні, за необхідності, розглядати можливість залучення інших експертів для виконання завдань.

1206.2 Фахівці з аудиту та підтвердження довіри до ІС повинні оцінювати та підтверджувати для інших експертів відповідність професійних кваліфікацій, компетенції, відповідного досвіду, ресурсів, незалежності та контролю якості процесів до початку виконання завдань.

1206.3 У рамках виконання своїх завдань фахівці з аудиту та підтвердження довіри до ІС повинні визначати, переглядати та оцінювати роботу інших експертів, а також документально оформляти висновки щодо обсягу залучення таких експертів і покладання на результати їх роботи.

1206.4 Фахівці з аудиту та підтвердження довіри до ІС повинні визначати, чи є робота інших експертів, які не є членами групи, що виконує завдання, достатньо адекватною та вичерпною для досягнення поточних цілей завдань, а також чітко документально оформляти свої висновки.

1206.5 Фахівці з аудиту та підтвердження довіри до ІС повинні визначати, чи можна вважати роботу інших експертів надійною і безпосередньо включати її або посилатися на неї у звіті.

1206.6 Фахівці з аудиту та підтвердження довіри до ІС повинні застосовувати додаткові процедури перевірки для отримання достатніх та відповідних доказів, якщо їх не надає робота інших експертів.

1206.7 Фахівці з аудиту та підтвердження довіри до ІС повинні надавати відповідні аудиторські оцінки або висновки та включати в них будь-які обмеження обсягу робіт, якщо необхідні докази не можна отримати за допомогою додаткових процедур перевірки.

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- розглядати залучення інших експертів до виконання завдань, якщо виникають обмеження (наприклад, необхідність певних технічних знань у зв'язку з характером поставлених задач, брак аудиторських ресурсів, часові обмеження), які можуть перешкоджати виконанню роботи або зменшити потенційні вигоди, що стосуються якості виконання завдань;
- документально оформляти вплив на досягнення цілей завдань, якщо неможливо залучити необхідних експертів, та включати певні задачі у план виконання завдань, щоб управляти ризиками та відповідати вимогам до доказів;
- враховувати незалежність інших експертів, залучаючи їх до роботи;
- мати доступ до всієї робочої та супровідної документації та звітів інших експертів, якщо це не суперечить правовому порядку;
- визначати обсяг залучення та оформляти висновки щодо ступеня покладання на результати роботи інших експертів, якщо такі експерти не мають доступу до записів згідно з правовим порядком;
- документально оформляти залучення інших експертів у звітах.

Терміни

Термін	Визначення
Інші експерти	Внутрішні та зовнішні у відношенні до організації, інші експерти можуть належати до: • аудиторів ІС із зовнішньої бухгалтерської фірми; • консультантів з питань управління; • експертів у предметній сфері завдання, призначених вищим виконавчим керівництвом компанії або групою.

Зв'язок із настановами

Тип	Назва
Настанова	2206 Залучення інших експертів

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1207 Невідповідності та незаконні дії

Положення

1207.1 При виконанні завдань фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики існування невідповідностей та незаконних дій.

1207.2 При виконанні завдань фахівці з аудиту та підтвердження довіри до ІС повинні дотримуватись позиції професійного скептицизму.

1207.3 Фахівці з аудиту та підтвердження довіри до ІС повинні документально оформляти та вчасно звітувати перед відповідними особами про будь-які суттєві невідповідності чи незаконні дії.

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- при плануванні та виконанні завдань зменшувати ризики аудиту до прийнятного рівня:
  - усвідомлюючи можливість існування значних помилок, проблем порушення контролів та недостовірностей у зв'язку з невідповідностями та незаконними діями, незалежно від оцінки ризиків невідповідностей та незаконних дій;
  - розуміючи організацію та її середовище, у тому числі внутрішні контролі, націлені на попередження чи виявлення невідповідностей та незаконних дій, що мають відношення до об'єкту перевірки, а також обсягу та цілей завдання;
  - отримуючи достатні та відповідні докази для визначення того, чи керівництво або інші співробітники організації знають про будь-які існуючі, припустимі або сумнівні невідповідності та незаконні дії;
- при виконанні аудиторських процедур розглядати незвичайні або неочікувані обставини, які можуть свідчити про ризик існування суттєвих помилок, проблем порушення контролів або недостовірностей у зв'язку з невідповідностями та незаконними діями;
- розробляти і виконувати процедури для перевірки відповідності внутрішніх контролів і ризику незастосування керівництвом контролів, націлених на попередження чи виявлення невідповідностей та незаконних дій;
- оцінювати, чи виявлені помилки, проблеми порушення контролів або недостовірності можуть свідчити про порушення та незаконні дії; якщо так, враховувати можливі наслідки відносно інших аспектів завдань і, зокрема, позицію керівництва;
- отримувати письмові звернення від керівництва щорічно або й частіше залежно від завдань, що:
  - підтверджують відповідальність керівництва за розробку і застосування внутрішніх контролів попередження та виявлення порушень і незаконних дій;
  - розкривають відповідні результати будь-яких оцінок ризиків, які свідчать про можливість існування помилок, проблем порушення контролів або недостовірностей внаслідок порушень і незаконних дій;
  - свідчать про знання керівництва про впливаючі на організацію порушення та незаконні дії, що стосуються керівництва та співробітників, які відіграють значну роль у внутрішніх контролях;
  - свідчать про знання керівництва про будь-які впливаючі на організацію сумнівні або припустимі порушення та незаконні дії зі звітів співробітників, колишніх співробітників, регуляторних органів та інших осіб;
- вчасно звітувати:
  - відповідному рівню керівництва про будь-яку виявлену або отриману інформацію щодо можливості існування суттєвих порушень і незаконних дій;
  - особам, відповідальним за корпоративне управління, про будь-які суттєві порушення та незаконні дії, що стосуються керівництва та співробітників, які відіграють значну роль у внутрішніх контролях;
- звітувати особам, відповідальними за корпоративне управління, про будь-які суттєві недоліки у розробці та застосуванні внутрішніх контролів, націлених на попередження та виявлення порушень і незаконних дій, виявлених під час виконання завдання, навіть якщо вони не входять в обсяг завдань;
- враховувати законодавчі та професійні вимоги до звітування, які застосовуються за таких обставин;
- розглядати відмову від виконання завдань, якщо суттєві помилки, проблеми порушення контролів, недостовірності або незаконні дії впливають на безперервне виконання завдань;
- документально оформляти усі звіти, планування, результати, оцінки та висновки щодо суттєвих порушень і незаконних дій, про які повідомлялось керівництво, особи, відповідальні за корпоративне управління, регуляторні органи та інші особи.

1207 Невідповідності та незаконні дії (продовження)

Терміни

Термін	Визначення
Порушення	Умови, які викликають погіршення або за яких послаблюється здатність досягати цілей аудиту. Порушення організаційної незалежності та індивідуальної об'єктивності може виникати внаслідок особистого конфлікту інтересів, обмеження обсягів, обмеження доступу до документів, персоналу, обладнання чи майна та обмеження ресурсів (таких як фінансування або кадрове забезпечення).
Професійний скептицизм	Ставлення, яке включає допитливе мислення та критичну оцінку аудиторських доказів. Джерело: AU 230.07, AICPA.
Суттєва недостовірність	Випадково або навмисно неправдиве твердження, що значною мірою впливає на результати аудиту

Зв'язок зі стандартами і настановами

Тип	Назва	
Стандарт	1008	Критерії
Стандарт	1202	Оцінювання ризиків у плануванні
Стандарт	1205	Докази
Настанова	2206	Залучення інших експертів
Настанова	2207	Невідповідності та незаконні дії

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

Стандарти звітування

Звіти, створені фахівцями з аудиту та підтвердження довіри до ІС, можуть різнитися залежно від типу завдань, які виконуються. Необхідно враховувати такі фактори: рівень підтвердження довіри, роботу фахівців з аудиту та підтвердження довіри до ІС в рамках аудиторської діяльності, надання ними прямих звітів щодо об'єкта перевірки чи звітів щодо тверджень, які стосуються об'єкта перевірки, а також ґрунтування звітів на результатах роботи, яка проводилась на рівні перевірки або експертизи.

Стандарти звітування:
1401 Звітування
1402 Подальша діяльність

Усі стандарти описані тут вичерпно. Визначення підкреслених слів наведені у розділі «Терміни». Посилання на окремі стандарти можна отримати на наступній сторінці: www.isaca.org/standard.

1401 Звітування

Положення

1401.1 Фахівці з аудиту та підтвердження довіри до ІС повинні звітувати про результати виконаних завдань, включаючи:

- **ідентифікацію організації, припустимого одержувача та будь-які обмеження щодо змісту та розповсюдження;**
- **обсяг, цілі та період виконання завдань, а також характер, визначення терміну проведення та обсягу роботи, що підлягає виконанню;**
- **результати, висновки та рекомендації;**
- **будь-які кваліфікації фахівців з аудиту та підтвердження довіри до ІС чи обмеження обсягу робіт, що стосуються виконання завдань;**
- **підпис, дату та розповсюдження згідно з умовами статуту аудиту та гарантійного листа.**

1401.2 Фахівці з аудиту та підтвердження довіри до ІС повинні гарантувати, що наведені в аудиторському звіті результати ґрунтуються на достатніх та відповідних аудиторських доказах.

Ключові аспекти

Фахівці з аудиту та підтвердження довіри до ІС повинні:

- отримувати від організації, що підлягає аудиту, відповідні письмові відомості, які чітко деталізують важливі сфери завдань, питання, що виникали, та їх вирішення, а також твердження, зроблені організацією, що підлягає аудиту;
- визначити, чи організація, що підлягає аудиту, підписала та продатувала свої відомості, щоб підтвердити прийняття нею обов'язків щодо завдань;
- документально оформляти та зберігати у робочій документації всі отримані під час проведення завдань звернення, як письмові, так і усні; для зменшення можливих непорозумінь отримувати від організації, що підлягає аудиту, аудиторські завдання на відповідність і звернення у письмовій формі;
- надавати звітам форму та зміст відповідно до вимог клієнта залежно від типу завдань, що виконуються, як, наприклад:
  – аудит (прямий чи атестаційний);
  – контроль (прямий чи атестаційний);
  – узгоджені процедури;
- описувати у звітах суттєві чи значні вразливі місця та їх вплив на досягнення цілей завдань;
- обговорювати з керівництвом зміст проектів звітів у предметній сфері до підготовки та публікування заключного звіту і, за необхідності, включати в заключний звіт відгуки керівництва щодо результатів, висновків та рекомендацій;
- звітувати особам, відповідальним за корпоративне управління, і, за необхідності, відповідальним повноважним особам про суттєві недоліки та значні порушення у контрольному середовищі; зазначати у звітах про таке інформування;
- посилатися на кожен окремий звіт у заключному звіті;
- звітувати керівництву організації, що підлягає аудиту, про внутрішні проблеми порушення контролів, які є меншими, ніж значущі, але більшими, ніж незначущі; у таких випадках необхідно повідомляти особам, відповідальним за корпоративне управління, або відповідальним повноважним особам про інформування керівництва організації, що підлягає аудиту, про такі внутрішні порушення контролів;
- визначати стандарти, які застосовуються при проведенні завдань; за необхідності, звітувати про будь-які невідповідності таким стандартам.

1401 Звітування(продовження)

Терміни

Термін	Визначення
Відповідна інформація	Інформація, що стосується контролів, надає оцінювачу змістовні дані про операції, пов'язані з базовими контролями або елементами системи контролів. Інформація, яка безпосередньо підтверджує функціонування контролів є найбільш відповідною. Інформація, яка опосередковано стосується функціонування контролів, також може бути відповідною, але менш відповідною, ніж безпосередня інформація. Дивіться про цілі якості інформації в COBIT 5.
Достатня інформація	Інформація вважається достатньою, якщо оцінювачі зібрали її у кількості, необхідній для формування обґрунтованого висновку. Щоб інформацію можна було вважати достатньою, перш за все вона повинна бути достовірною. Дивіться про цілі якості інформації в COBIT 5.
Достовірна інформація	Інформація, яка є відповідною (тобто відповідає визначеній цілі), надійною (тобто така, яка є точною, може бути перевірена та отримана від об'єктивного джерела) та своєчасною (тобто отриманою і використаною в належні часові рамки). Дивіться про цілі якості інформації в COBIT 5.
Надійна інформація	Інформація з об'єктивного джерела, яка є точною, і може бути підтверджена. Дивіться про цілі якості інформації в COBIT 5.
Своєчасна інформація	Інформація, отримана і використана у такі часові проміжки, які дозволили попередити або виявити проблеми порушення контролю до того, як вони стали суттєвими для організації.

Зв'язок із настановами

Тип	Назва
Настанова	2401 Звітування

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

1402 Подальша діяльність

Положення

1402.1 Фахівці з аудиту та підтвердження довіри до ІС повинні проводити моніторинг відповідної інформації, щоб зробити висновок, чи керівництво своєчасно запланувало / вжило необхідні заходи для розгляду результатів і рекомендацій аудиторського звіту.

Ключові аспекти

Функція внутрішнього аудиту повинна встановити процес подальшого контролю,щоб простежити та переконатися в тому, що заходи керівництва були ефективно впроваджені, або вище виконавче керівництво прийняло ризик незастосування заходів. Зовнішні фахівці з аудиту та підтвердження довіри до ІС можуть покладатися на функцію внутрішнього аудиту і слідувати узгодженим рекомендаціям залежно від обсягу та умов завдань.

Зв'язок із настановами

Тип	Назва
Настанова	2402 Подальша діяльність

Дата набуття чинності

Цей стандарт ISACA є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з 1 листопада 2013 року.

2. Настанови з аудиту та підтвердження довіри до ІС

Розділ 2000 розглядає настанови, що обґрунтовують наступні стандарти:
2000 Загальні настанови
2200 Настанови виконання
2400 Настанови звітування

Кожен підрозділ розділу про настанови орієнтується на:
- питання і процеси щодо ІС, які фахівці з аудиту та підтвердження довіри до ІС повинні розуміти та враховувати, розглядаючи планування, визначення обсягу, виконання завдань і звітування щодо діяльності в галузі аудиту та підтвердження довіри до ІС;
- процеси, процедури, методи та підходи до аудиту та підтвердження довіри до ІС, які фахівці з аудиту та підтвердження довіри до ІС повинні враховувати у своїй діяльності в галузі аудиту та підтвердження довіри до ІС.

Загальні настанови

Загальні настанови:
2001 Статут аудиту
2002 Організаційна незалежність
2003 Професійна незалежність
2004 Обґрунтовані очікування
2005 Належна професійна ретельність
2006 Професійність
2007 Твердження
2008 Критерії

Усі настанови описані тут вичерпно. Посилання на окремі стандарти можна отримати на наступній сторінці: www.isaca.org/standard.

2001 Статут аудиту

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівець»

1.1 Мета

1.1.1 Мета цієї настанови полягає у тому, щоб сприяти фахівцям з аудиту та підтвердження довіри до ІС у підготовці статуту аудиту, який визначає мету, обов'язки, повноваження та підзвітність функції аудиту та підтвердження довіри до ІС.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1	Стандарт 1001	Статут аудиту
1.2.2	Стандарт 1002	Організаційна незалежність
1.2.3	Стандарт 1003	Професійна незалежність

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані із завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Накази
2.2 Зміст статуту аудиту

2.1 Накази

2.1.1 Фахівці повинні отримувати чіткі накази щодо виконання функції аудиту. Як правило, ці накази документально оформляються у статуті аудиту, який офіційно затверджується особами, відповідальними за корпоративне управління, наприклад, радою директорів та аудиторським комітетом. Якщо статут аудиту розроблений для функції аудиту в цілому, у нього необхідно включати накази щодо аудиту та підтвердження довіри до ІС.

2.2 Зміст статуту аудиту

2.2.1 Статут аудиту повинен чітко описувати такі чотири аспекти: призначення, обов'язки, повноваження та підзвітність. Ці аспекти викладені у наступних підрозділах.

2.2.2 Наступні підрозділи містять таку інформацію про мету статуту аудиту та функції аудиту:
- мета / завдання статуту аудиту окреслює функціональні та організаційні стандарти функції аудиту;
- формулювання місії та цілі функції аудиту допомагає структурно підходити до оцінювання і покращення розробки та операційної ефективності процесів управління ризиками, системи внутрішніх контролів і структур управління інформаційними системами;
- обсяг функції аудиту визначається для організації в цілому або її окремої структури;
- корпоративне управління детально описує повноважні органи для статуту та аудиту.

2.2.3 Наступні підрозділи містять таку інформацію про обов'язки функції аудиту:
- принципи діяльності надають більш детальний і кількісний перелік різних цілей функції аудиту;
- незалежність детально описує застосування вимог функції аудиту і фахівців до незалежності згідно зі Стандартом 1002 «Організаційна незалежність» і Стандартом 1003 «Професійна незалежність»;
- відносини із зовнішнім аудитом детально описують зв'язок функції аудиту із зовнішніми

2001 Статут аудиту (продовження)

2.2 Зміст статуту аудиту (продовження)

аудиторами:
- – зустрічі із зовнішніми аудиторами для координації робочих зусиль з метою мінімізації подвійної роботи;
- – забезпечення доступу до робочих документів, документації та доказів фахівців;
- – врахування роботи, запланованої зовнішніми аудиторами, при складанні плану аудиту на наступний період;
- • очікування організації, що підлягає аудиту, детально описують, які послуги та результати може очікувати організація, що підлягає аудиту, від функції аудиту і фахівців:
- – опис виявлених проблем, їх наслідків і можливих рішень стосовно сфери відповідальності організації, що підлягає аудиту;
- – можливість включення до аудиторського звіту пропозицій щодо реагування керівництва та корегуючих заходів, які можуть бути застосовані після отримання результатів; це може включати посилання на відповідні договори про рівень обслуговування (SLA) для таких складових, як звіти про надання послуг, реагування на скарги організації, що підлягає аудиту, якість послуг, перегляд ефективності, процес звітування та узгодження результатів;
- • вимоги організації, що підлягає аудиту, детально описують її обов'язки, наприклад, забезпечення доступу до неї та сприяння у виконанні обов'язків функції аудиту і фахівців;
- • надання інформації організації, що підлягає аудиту, детально описує частоту та канали комунікації функції аудиту з організацією, що підлягає аудиту.

2.2.4 Наступні підрозділи містять таку інформацію про повноваження функції аудиту:
- • фахівці, які виконують завдання з аудиту, отримують право доступу до відповідної інформації, систем, персоналу та приміщень організації; функція аудиту здійснюється фахівцями, які:
- – отримують санкціонований, повний, вільний та необмежений доступ до всіх без винятку записів, документації, систем і приміщень організації та допомогу вищого виконавчого керівництва в отриманні такого доступу;
- – мають право отримувати інформацію від співробітників, консультантів та підрядників організації;
- • необхідно враховувати обмеження повноважень функції аудиту і фахівців, якщо такі існують;
- • функція аудиту має право визначати, які процеси підлягають аудиту, наприклад, вона вільно може обирати, які процеси піддавати аудиту на основі ризик-орієнтованого плану аудиту.

2.2.5 Наступні підрозділи містять таку інформацію про підзвітність функції аудиту:
- • організаційна структура, включаючи лінії звітування перед радою та вищим виконавчим керівництвом, повинна, наприклад, забезпечувати відкритий і необмежений доступ функції аудиту до ради та її членів;
- • звітування детально описує формат, зміст та одержувачів звітів щодо результатів кожного завдання з аудиту, наприклад, після виконання кожного завдання з аудиту функція аудиту видає та надає відповідним зацікавленим сторонам письмовий аудиторський звіт, що описує обсяг, вжиті заходи, результати, рекомендації, реагування та корегуючі заходи, вжиті керівництвом;
- • ефективність функції аудиту детально описує процес періодичного звітування раді згідно з планом аудиту та в рамках бюджету, наприклад, щоквартальне звітування функції аудиту раді щодо цілей, обов'язків і повноважень, а також щодо ефективності згідно з планом аудиту і в рамках бюджету;
- • відповідність стандартам детально описує стандарти, яких дотримується функція аудиту і фахівці, наприклад, функція аудиту і фахівці дотримуються та діють відповідно до всіх стандартів та положень ISACA щодо аудиту та підтвердження довіри до ІС;
- • процес забезпечення довіри (наприклад, опитування, дослідження рівня задоволення клієнтів або довіри до виконання завдань) гарантує розуміння функцією аудиту потреб та очікувань організації, що підлягає аудиту; ці потреби оцінюються згідно зі статутом аудиту і націлені на вдосконалення послуг або, за необхідності, на зміну послуг чи статуту аудиту; незалежна зовнішня перевірка довіри дозволяє функції аудиту оцінювати її відповідність стандартам, основним положенням організації щодо ризиків і контролю, оптимального використання ресурсів і застосування передового досвіду; щоб відповідати стандартам ISACA щодо аудиту та підтвердження довіри до ІС, незалежна зовнішня перевірка довіри до функції аудиту повинна виконуватися щонайменше через кожних п'ять років;
- • необхідно встановлювати правила кадрового забезпечення для виконання завдань з аудиту, наприклад, визначати мінімальні часові рамки, раніше яких не можна давати фахівцям

2001 Статут аудиту (продовження)

2.2 Зміст статуту аудиту (продовження)

завдання з аудиту у тих сферах, в яких вони надавали неаудиторські послуги, оскільки це може обмежувати незалежність; статут аудиту також повинен визначати можливість залучення фахівців до надання неаудиторських послуг, а також у загальних рисах характер, терміни виконання та обсяг таких послуг, щоб гарантувати, що незалежність не обмежується; це може зменшити чи мінімізувати потребу отримання конкретних розпоряджень для надання неаудиторських послуг у кожному конкретному випадку;

- функція аудиту повинна постійно підвищувати кваліфікацію фахівців, наприклад, вона зобов'язана щорічно забезпечувати фахівцям щонайменше 40 годин підготовки;
- необхідно вживати узгоджені заходи щодо функції аудиту і поведінки фахівців, наприклад, штрафи у випадку невиконання обов'язків будь-якою зі сторін.

2.2.6 Інші аспекти, які необхідно враховувати при формуванні статуту аудиту:

- перевірка та внесення змін у статут, що є обов'язком функції аудиту; необхідно періодично оцінювати чи мета, обов'язки, повноваження та підзвітність, визначені у статуті аудиту, є адекватними, та повідомляти про результати такого оцінювання аудиторський комітет;
- затвердження змін, внесених у статут аудиту, особами, відповідальними за корпоративне управління;
- включення у статут супровідних документів, у тому числі посилань на відповідні стандарти, настанови, політики, основні положення, посібники тощо.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами
3.2 Зв'язок із процесами COBIT 5
3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA щодо аудиту та підтвердження довіри до ІС, які безпосередньо обґрунтовуються цією настановою;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1001 Статут аудиту	Функція аудиту та підтвердження довіри до ІС повинна належним чином документувати у статуті аудиту функцію аудиту, зазначаючи цілі, обов'язки, повноваження та підзвітність. Функція аудиту та підтвердження довіри до ІС повинна мати статут аудиту, попередньо узгоджений і затверджений на відповідному рівні організації.
1002 Організаційна незалежність	Для забезпечення об'єктивності при виконанні завдань з аудиту та підтвердження довіри функція аудиту та підтвердження довіри до ІС повинна бути незалежною від сфери та типу діяльності, що перевіряються.
1003 Професійна незалежність	Фахівці з аудиту та підтвердження довіри до ІС повинні бути незалежними та об'єктивними у своїх ставленнях і проявах у всіх питаннях, які стосуються виконання завдань з аудиту та підтвердження довіри.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:

- процеси COBIT 5;
- призначення процесів COBIT 5.

Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

2001 Статут аудиту (продовження)

3.2 Зв'язок із процесами COBIT 5 (продовження)

Процес COBIT 5	Призначення процесу
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
- у колег, що працюють в організації;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- у професійних організаціях;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Завдання з аудиту	Конкретне аудиторське завдання, задача або перевірка, як, наприклад, аудит, перевірка контролю, самооцінювання, розслідування фактів шахрайства або надання консультацій. Завдання з аудиту може включати різноманітні задачі або дії, спрямовані на досягнення певної низки пов'язаних цілей.
Незалежність	Свобода від обставин, що загрожують об'єктивності чи створюють враження об'єктивності. Необхідно, щоб такі загрози об'єктивності нейтралізувалися на рівні окремого аудитора, завдання і на функціональному та організаційному рівнях. Незалежність включає в себе незалежність у поглядах і незалежність у проявах.
Статут аудиту	Документ, затверджений особами, відповідальними за корпоративне управління, що визначає мету, повноваження та відповідальність щодо дій внутрішнього аудиту. Статут повинен: • встановлювати роль внутрішнього аудиту в організації; • санкціонувати доступ до документації, персоналу та майна, необхідних для виконання завдань з аудиту ІС та підтвердження довіри до ІС; • визначати сферу діяльності аудиту.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2002 Організаційна незалежність

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови – розгляд незалежності функції аудиту та підтвердження довіри до ІС в організації. Необхідно враховувати три важливі аспекти:
- роль функції аудиту та підтвердження довіри до ІС в організації;
- рівень підзвітності функції аудиту та підтвердження довіри до ІС в організації;
- надання керівництвом та фахівцям з аудиту та підтвердження довіри до ІС неаудиторських послуг організації.

1.1.2 Ця настанова регулює оцінювання організаційної незалежності та детально описує зв'язок між організаційною незалежністю і статутом аудиту та планом аудиту.

1.1.3 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1001 Статут аудиту
1.2.2 Стандарт 1002 Організаційна незалежність
1.2.3 Стандарт 1003 Професійна незалежність
1.2.4 Стандарт 1004 Обґрунтовані очікування
1.2.5 Стандарт 1006 Професійність

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані із завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Роль в організації
2.2 Рівень підзвітності
2.3 Неаудиторські послуги
2.4 Оцінювання незалежності
2.5 Статут аудиту та план аудиту

2.1 Роль в організації

2.1.1 Для забезпечення організаційної незалежності функція аудиту повинна відігравати таку роль в організації, яка дозволятиме їй виконувати свої обов'язки без завад. Цього можна досягти:
- якщо згідно зі статутом аудиту функція аудиту буде незалежною функцією чи відділом поза межами організаційних відділів; функція аудиту не повинна виконувати жодних операційних обов'язків чи діяльності;
- якщо функція аудиту буде звітувати такому рівню керівництва в організації, який може забезпечити організаційну незалежність; звітування керівнику операційного відділу може скомпрометувати організаційну незалежність, що більш детально описано у підрозділі 2.2.

2002 Організаційна незалежність (продовження)

2.1 Роль в організації (продовження)

2.1.2 Функція аудиту повинна уникати виконання неаудиторських ролей в ініціативах, пов'язаних з ІС, що вимагають прийняття на себе керівних обов'язків, оскільки у майбутньому це може обмежувати незалежність. Незалежність та підзвітність функції повинні регулюватися у статуті аудиту, як зазначено у Стандарті 1001 «Статут аудиту».

2.2 Рівень підзвітності

2.2.1 Функція аудиту повинна звітувати такому рівню керівництва в організації, який забезпечує її повну організаційну незалежність. Незалежність повинна бути прописана у статуті аудиту та повинна регулярно, не рідше ніж один раз на рік, підтверджуватися в раді директорів та осіб, відповідальних за корпоративне управління.

2.2.2 Для забезпечення організаційної незалежності функції аудиту з метою отримання побажань та / або затвердження осіб, відповідальних за корпоративне управління, (наприклад, ради директорів) необхідно звітувати про:
- планування ресурсів і бюджету;
- (ризик-орієнтований) план аудиту;
- подальший контроль ефективності функції аудиту в галузі аудиту ІС;
- подальший контроль значущих обмежень обсягу та ресурсів.

2.2.3 Для забезпечення організаційної незалежності функції аудиту необхідна повна підтримка ради та вищого виконавчого керівництва.

2.3 Неаудиторські послуги

2.3.1 У багатьох організаціях керівництво і персонал, що працює в галузі ІС, очікують, що функцію аудиту можна залучати до надання неаудиторських послуг, наприклад, до участі фахівців в ініціативах, пов'язаних з ІС, протягом повного чи неповного робочого дня, або до виконання проектними групами, які займаються ІС, консультативних чи консалтингових завдань.

2.3.2 Діяльність, яка є рутинною та адміністративною або стосується питань, які загалом є незначущими, не вважається пов'язаною з керівними обов'язками і, таким чином, не обмежує незалежність. До неаудиторських послуг, які також не обмежують незалежність чи об'єктивність, якщо вживаються адекватні запобіжні заходи, відносяться рутинні консультації, що надають інформацію про технологічні ризики та контролі.

2.3.3 Нижче наведені неаудиторські послуги, які обмежують незалежність та об'єктивність, оскільки загрози, які вони створюють, є настільки значущими, що жодні запобіжні заходи не зможуть зменшити їх до прийнятного рівня:
- прийняття на себе керівних обов'язків чи виконання керівної діяльності;
- значне залучення фахівців до контролю та роботи, пов'язаної з розробкою, тестуванням, встановленням, налаштуванням або діяльністю інформаційних систем, які є суттєвими або значними для об'єкта перевірки у завданнях з аудиту чи підтвердження довіри;
- розробка контролів для інформаційних систем, які є суттєвими або значними для об'єкта перевірки у поточних чи запланованих завданнях з аудиту;
- виконання ролі, пов'язаної з корпоративним управлінням, коли фахівці несуть індивідуальну чи колективну відповідальність за прийняття рішень керівництва або затвердження політик і стандартів;
- консультування, яке є основою для рішень керівництва.

2.3.4 Надання неаудиторських послугу сферах, які зараз є або у майбутньому будуть об'єктом перевірки у завданнях з аудиту, також створює загрози незалежності, які важко подолати за допомогою запобіжних заходів. У такому випадку після надання неаудиторських послуг у цих сферах може скластися враження про порушення незалежності та об'єктивності функції аудиту і фахівців. Функція аудиту і фахівці повинні визначати, чи можна вжити адекватні запобіжні заходи, щоб у достатньому обсязі зменшити ці загрози незалежності, які є реальними або сприймаються як такі.

2.3.5 Більш детальні вказівки щодо подолання таких загроз незалежності наведені у Стандарті 1003 «Професійна незалежність» та пов'язаній з ним Настанові 2003.

2.4 Оцінювання незалежності

2.4.1 Функція аудиту і фахівці повинні регулярно оцінювати незалежність. Згідно зі Стандартом 1003 «Професійна незалежність» функція аудиту повинна виконувати таке оцінювання щорічно, а фахівці – перед виконанням кожного завдання. При оцінюванні необхідно враховувати наступні фактори:
- зміни в особистих відносинах;

2002 Організаційна незалежність (продовження)

2.4 Оцінювання незалежності (продовження)

- фінансові інтереси;
- попередні робочі завдання та обов'язки.

2.4.2 Необхідно, щоб функція аудиту інформувала та обговорювала з радою директорів або особами, відповідальними за корпоративне управління, можливі питання, пов'язані з організаційною незалежністю. Необхідно вирішувати такі питання та вносити відповідні рішення у статут аудиту або план аудиту.

2.5 Статут аудиту та план аудиту

2.5.1 В аспектах, пов'язаних з відповідальністю, статут аудиту повинен детально описувати реалізацію організаційної незалежності функції аудиту. Окрім того, статут аудиту повинен розглядати можливі порушення незалежності.

2.5.2 Організаційна незалежність повинна також розглядатися в плані аудиту. Необхідно, щоб функція аудиту могла визначати обсяг плану незалежно, без обмежень з боку вищого виконавчого керівництва.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами
3.2 Зв'язок із процесами COBIT 5
3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA щодо аудиту та підтвердження довіри до ІС, які безпосередньо обґрунтовуються цією настановою;
- положення стандартів, які є найбільш придатні для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1001 Статут аудиту	Функція аудиту та підтвердження довіри до ІС повинна належним чином документувати у статуті аудиту функцію аудиту, зазначаючи цілі, обов'язки, повноваження та підзвітність. Функція аудиту та підтвердження довіри до ІС повинна мати статут аудиту, попередньо узгоджений і затверджений на відповідному рівні організації.
1002 Організаційна незалежність	Для забезпечення об'єктивності при виконанні завдань з аудиту та підтвердження достовірності функція аудиту та підтвердження довіри до ІС повинна бути незалежною від сфери та типу діяльності, що перевіряються.
1003 Професійна незалежність	Фахівці з аудиту та підтвердження довіри до ІС повинні бути незалежними та об'єктивними у своїх ставленнях і проявах у всіх питаннях, які стосуються виконання завдань з аудиту та підтвердження довіри.
1004 Обґрунтовані очікування	Фахівці з аудиту та підтвердження довіри до ІС повинні мати обґрунтовані очікування щодо обсягу завдань, який має бути таким, щоб забезпечити надання висновку про об'єкт перевірки та вирішити питання, пов'язані з будь-якими обмеженнями.
1006 Професійність	Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні колективно володіти необхідними навичками і проявляти професійність при виконанні завдань з аудиту та підтвердження довіри до ІС, а також бути професійно компетентними для здійснення роботи.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:

- процеси COBIT 5;
- призначення процесів COBIT 5.

Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

2002 Організаційна незалежність (продовження)

3.2 Зв'язок із процесами COBIT 5 (продовження)

Процес COBIT 5	Мета процесу
EDM01 Забезпечити впровадження та підтримку основних положень корпоративного управління	Забезпечити єдиний підхід, інтегрований та узгоджений з підходом організації до корпоративного управління. Приймати такі рішення у сфері IT, які відповідатимуть стратегіям і цілям організації. Здійснювати ефективний і прозорий нагляд за процесами, пов'язаними з IT, та підтверджувати їх відповідність законодавчим і регулятивним вимогам, а також забезпечити дотримання членами керівної ради вимог до корпоративного управління.
APO01 Управляти основними положеннями управління IT	Забезпечити єдиний підхід до управління, що гарантуватиме виконання вимог до корпоративного управління, які охоплюють процеси управління, організаційні структури, ролі та обов'язки, надійну і стабільну діяльність, навички та компетенції.
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
- у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Незалежність	Свобода від обставин, що загрожують об'єктивності чи створюють враження об'єктивності. Необхідно, щоб такі загрози об'єктивності нейтралізувалися на рівні окремого аудитора, завдання і на функціональному та організаційному рівнях. Незалежність включає в себе незалежність у поглядах і незалежність у проявах.
Об'єктивність	Здатність неупереджено висловлювати судження, робити висновки та давати рекомендації.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2003 Професійна незалежність

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Посилання та встановлення відповідності
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови полягає у наданні фахівцям з аудиту та підтвердження довіри до ІС основних положень, що стосуються:
- визначення умов, за яких незалежність може бути обмеженою або сприйматися як така;
- розгляду потенційних альтернативних підходів до таких аудиторських процесів, при яких незалежність може бути обмеженою або сприйматися як така;
- зменшення чи усунення впливу на незалежність фахівців з аудиту та підтвердження довіри до ІС, які надають неаудиторські послуги або виконують неаудиторські ролі або функції;
- визначення вимог розкриття інформації, якщо незалежність є обмеженою, або може сприйматися як така.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1002 Організаційна незалежність
1.2.2 Стандарт 1003 Професійна незалежність
1.2.3 Стандарт 1005 Належна професійна ретельність

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані із завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Концептуальні основні положення
2.2 Загрози та запобіжні заходи
2.3 Управління загрозами
2.4 Неаудиторські послуги та ролі
2.5 Неаудиторські послуги та ролі, які не обмежують незалежність
2.6 Неаудиторські послуги та ролі, які обмежують незалежність
2.7 Відповідність незалежності при наданні неаудиторських послуг чи виконанні неаудиторських ролей
2.8 Корпоративне управління припустимістю неаудиторських послуг і ролей
2.9 Звітування

2.1 Концептуальні основні положення

2.1.1 При оцінці загроз незалежності можуть бути доречними багато різних обставин чи їх комбінацій. Неможливо визначити кожну ситуацію, в якій виникає загроза незалежності і встановити відповідні запобіжні заходи. Таким чином, ця настанова встановлює лише концептуальні основні положення і тільки фахівець визначає, оцінює та розглядає загрози незалежності. Підхід, що ґрунтується на концептуальних основних положеннях, сприяє дотриманню стандартів щодо незалежності та розглядає багато різних комбінацій обставин, за яких виникають загрози незалежності.

2.1.2 Підхід, що ґрунтується на концептуальних основних положеннях, застосовується фахівцями для:

2003 Професійна незалежність (продовження)

2.1 Концептуальні основні положення (продовження)

- визначення загроз незалежності;
- оцінювання значущості виявлених загроз;
- за необхідності, вживання запобіжних заходів для усунення загроз чи їх зменшення до прийнятного рівня.

2.1.3 Якщо фахівці визначають, що відповідні запобіжні заходи недоступні або не можуть бути застосованими для усунення загрози чи її зменшення до прийнятного рівня, вони повинні усунути обставини чи відносини, за яких виникають загрози, або припинити чи відмовитись від завдання з аудиту та підтвердження довіри. Якщо фахівці не можуть припинити чи відмовитись від завдання, вони повинні розкрити інформацію про порушення незалежності особам, відповідальним за корпоративне управління, та у всіх звітах про результати завдань.

2.1.4 При застосовуванні цих концептуальних основних положень фахівці повинні враховувати свої професійні судження.

2.1.5 Важливим аспектом при застосуванні цих основних положень є консультування. Фахівці з аудиту та підтвердження довіри до ІС повинні, за необхідності, звертатися до інших настанов, які можна знайти:

- у колег, що працюють в організації;
- у керівництва;
- в осіб, відповідальних за корпоративне управління;
- у відповідних професійних організаціях.

2.1.6 Хоча перед фахівцями не стоїть вимога бути незалежними при наданні неаудиторських послуг та виконанні неаудиторських ролей, об'єктивність залишається необхідною професійною вимогою. При наданні неаудиторських послуг та виконанні неаудиторських ролей фахівці повинні розглядати застосування цих концептуальних основних положень, визначаючи загрози об'єктивності, оцінюючи значущість таких загроз і вживаючи відповідні запобіжні заходи.

2.2 Загрози та запобіжні заходи

2.2.1 Загрози можуть виникати внаслідок багатьох відносин та обставин. Якщо певна обставина чи відносини створюють загрозу, вони можуть обмежувати чи створювати враження порушення професійної незалежності. Певна обставина чи відносини можуть створити більше, ніж одну загрозу незалежності. Загрози підпадають під одну чи кілька наступних категорій:

- **особисті інтереси** – загроза того, що фінансовий чи інший інтерес може невідповідним чином вплинути на професійні судження чи поведінку;
- **самоконтроль** – загроза того, що фахівці не будуть належним чином оцінювати результати попереднього професійного судження чи послуги, наданої ними чи іншими особами, які відносяться до функції аудиту, на яку покладатимуться фахівці при формуванні свого професійного судження під час виконання поточних завдань;
- **захист інтересів** – загроза того, що фахівці можуть підтримувати позицію організації, що підлягає аудиту, настільки, що може скомпрометуватися їхня професійна об'єктивність;
- **близькі знайомства** – загроза того, що внаслідок довгих чи тісних відносин з організацією, що підлягає аудиту, фахівці будуть занадто прихильними до інтересів організації, що підлягає аудиту, або будуть занадто легко приймати роботу, погляди та докази організації, що підлягає аудиту;
- **залякування** – загроза того, що внаслідок тиску, який є реальним чи сприймається як такий, у тому числі внаслідок спроб чинити неналежний вплив на фахівців, вони будуть утримуватися у своїй роботі від цілісності та об'єктивності;
- **упередження** – загроза того, що внаслідок політичних, ідеологічних, соціальних, психологічних або інших переконань фахівці займуть необ'єктивну позицію;
- **участь у керівництві** – загроза, яка виникає, коли фахівці приймають на себе керівні ролі або будь-яким іншим чином виконують керівні функції від імені установи, яка підлягає аудиту чи підтвердженню довіри.

2.2.2 Запобіжні заходи – це контролі, розроблені для усунення загроз незалежності або їх зменшення до прийнятного рівня. Згідно із концептуальними основними положеннями фахівці застосовують запобіжні заходи до певних фактів чи обставин, за яких існують загрози незалежності. У деяких випадках для вирішення загрози необхідно застосувати багато запобіжних заходів.

Приклади запобіжних заходів, які можуть розглядати фахівці у відповідь на виявлені загрози:

- структура корпоративного управління в організації та функції аудиту, які забезпечують належний нагляд і звітування щодо послуг з аудиту та підтвердження довіри до ІС;
- звітування фахівцями (та керівництвом аудиту ІС) відповідному рівню керівництва організації,

2003 Професійна незалежність (продовження)

2.2 Загрози та запобіжні заходи (продовження)

краще – особам, відповідальним за корпоративне управління;
- внутрішні процедури організації та функції аудиту, які забезпечують об'єктивність вибору при дорученні завдань, наприклад, адекватні вимоги до освіти, підготовки та досвіду, а також до підвищення кваліфікації;
- залучення керівництва та персоналу, які є зовнішніми щодо функції аудиту, як, наприклад, залучення, окрім фахівців, персоналу з іншої функції, відділу або зовнішньої організації;
- адекватна система заохочень (винагород і штрафів), яка винагороджує фахівців за критичне об'єктивне мислення та штрафує їх за упередження або необ'єктивність;
- періодична ротація фахівців при виконанні завдань з аудиту ІС з метою зменшення загроз внаслідок близьких знайомств чи самоконтролю;
- адекватні практики найму персоналу, як, наприклад, перевірка даних та відбір, які можуть збільшити ймовірність того, що фахівці будуть неупередженими та не матимуть особистих інтересів;
- усунення особи з групи, яка займається аудитом ІС, якщо інтереси чи відносини цієї особи можуть загрожувати незалежності;
- належні вимоги до ведення документації та звітування, що забезпечують документальне оформлення оцінювання професійної незалежності у робочій документації та, відповідно, у звітній документації;
- ретельна перевірка виконаної роботи співробітником чи керівництвом, які входять у функцію аудиту, але не є членами групи,що займається аудитом ІС;
- залучення незалежного ресурсу з функції аудиту або інших вищезазначених джерел для проведення незалежного зовнішнього контролю довіри до аудиту або для виконання ролі незалежного спостерігача при плануванні, виконанні роботи на території клієнта і звітуванні;
- зовнішня перевірка звітів, повідомлень та інформації, наданих фахівцями, загальновизнаною третьою стороною, наприклад, визнаним у цій сфері повноважним органом або незалежним фахівцем;
- передача завдання з аудиту та підтвердження довіри до ІС зовнішньому постачальнику послуг.

2.3 Управління загрозами

2.3.1 Факти і обставини, які створюють загрози незалежності, можуть виникати внаслідок таких подій, як початок нового аудиту, залучення нового персоналу до поточного аудиту та прийняття неаудиторських послуг в установі, яка підлягає аудиту. Загрози незалежності можуть виникнути внаслідок багатьох інших подій. Як тільки у фахівців з'являється нова відповідна інформація про загрозу незалежності під час виконання завдань з аудиту та підтвердження довіри, вони повинні провести повторне оцінювання значущості загрози у відповідності до концептуальних основних положень.

2.3.2 Фахівці повинні оцінювати загрози:
- незалежності у відповідності до концептуальних основних положень, якщо факти та обставини, за яких фахівці виконують свою роботу, можуть створювати нові загрози або збільшувати значущість існуючих загроз незалежності;
- як індивідуально, так і в сукупності, оскільки загрози можуть мати сукупний ефект на професійну незалежність;
- з позиції як довіри до ІС, так і кількості, визначаючи значущість загрози.

2.3.3 Функція аудиту і фахівці повинні визначати, чи є виявлені загрози незалежності на прийнятному рівні, а також чи були вони усунені чи зменшені до прийнятного рівня. Загроза незалежності неприйнятна, якщо вона може:
- впливати на здатність фахівців виконувати завдання з аудиту та підтвердження довіри, не зазнаючи впливів, які можуть скомпрометувати їхні професійні судження;
- ставити фахівців, функцію аудиту або аудиторську організацію перед обставинами, за яких розсудлива інформована третя особа може дійти висновку про компрометацію цілісності, об'єктивності чи професійного скептицизму аудиторської організації або члена групи, яка займається аудитом та підтвердженням довіри до ІС.

2.3.4 Якщо функція аудиту і фахівці виявляють загрози незалежності і на основі оцінювання таких загроз визначають, що їх рівень неприйнятний, вони повинні:
- встановити, чи доступні відповідні запобіжні заходи, і чи можна застосовувати їх для усунення або зменшення загроз до прийнятного рівня;
- при встановленні вищевказаного застосовувати свої професійні судження, дотримуючись незалежності у поглядах і незалежності у проявах;

2003 Професійна незалежність (продовження)

2.3 Управління загрозами (продовження)

- згідно із пунктом 2.1.5 звертатися до інших настанов, які можна знайти у відповідних сторін, для визначення та застосування необхідних запобіжних заходів.

2.3.5 При формуванні висновків щодо відповідності вимогам до незалежності докази, що відносяться до суджень фахівців, можна отримати у документації.

2.3.6 Фахівці разом із керівництвом аудиту та, за необхідності, особами, відповідальними за корпоративне управління, повинні документально оформляти висновки щодо відповідності вимогам до незалежності та суті будь-яких відповідних рішень, що обґрунтовують такі висновки, включаючи:

- кроки, зроблені для аналізу характеру незалежності;
- реальний характер питань, пов'язаних із незалежністю;
- перелік та опис загроз;
- заключні висновки;
- відповідні запобіжні заходи для усунення чи зменшення загроз до прийнятного рівня.

2.4 Неаудиторські послуги та ролі

2.4.1 У багатьох організаціях керівництво, персонал, що займається ІС, та внутрішній аудит очікують, що фахівців можна залучати до надання таких неаудиторських послуг і виконання таких неаудиторських ролей, як:

- визначення стратегій ІС, пов'язаних з такими сферами, як технології, прикладні програми та ресурси;
- оцінювання, підбір і застосування технологій;
- оцінювання, підбір, налаштування та застосування прикладних програм і рішень третіх сторін;
- планування, розробка та застосування прикладних програм і рішень, пов'язаних з ІС, що готуються на замовлення;
- застосування передового досвіду, політик і процедур, пов'язаних з різними функціями ІТ;
- планування, розробка, тестування та застосування безпеки та контролів, пов'язаних з ІТ;
- управління проектами, пов'язаними з ІТ.

2.4.2 Загалом, надання неаудиторських послуг і виконання неаудиторських ролей передбачає участь в ініціативах, пов'язаних з ІС, протягом повного чи неповного робочого дня, або виконання проектними групами, які займаються ІС, консультативних чи консалтингових завдань. Фахівці з аудиту та підтвердження довіри до ІС можуть виконувати неаудиторську функцію наступним чином:

- займаючись тимчасовими завданнями протягом повного робочого дня або залучаючи персонал, що працює над аудитом та підтвердженням довіри до ІС, до роботи проектних груп, які займаються ІТ;
- залучаючи членів персоналу, які займаються аудитом та підтвердженням довіри до ІС, протягом неповного робочого дня до роботи різних проектних структур, пов'язаних з ІТ, як, наприклад, керівних чи робочих груп проекту, а також груп по оцінюванню, переговорах, виконанню контрактних чи проектних робіт, контролю довіри і виявленню та усуненню помилок;
- виконуючи роль радника чи експерта проектів чи контролів ІТ на тимчасовій основі.

2.4.3 Надання неаудиторських послуг та виконання неаудиторських ролей може створювати загрози професійної незалежності у ставленнях чи проявах, що особливо важко подолати за допомогою запобіжних заходів, якщо сфера, у якій надавалися неаудиторські послуги та виконувалися неаудиторські ролі, зараз є або у майбутньому стане об'єктом перевірки завдання з аудиту та підтвердження довіри. У такій ситуації при наданні неаудиторських послуг та виконанні неаудиторських ролей може скластися враження порушення як незалежності, так і об'єктивності фахівців.

2.4.4 Фахівці, які надають неаудиторські послуги та виконують неаудиторські ролі, повинні оцінити за допомогою концептуальних основних положень, чи такі неаудиторські послуги або ролі створюють обмеження незалежності у ставленнях чи проявах для поточних чи майбутніх завдань з аудиту та підтвердження довіри. Це стосується тих завдань, у яких сфера надання неаудиторських послуг і виконання неаудиторських ролей характеризується значущістю або суттєвістю об'єкта перевірки або зацікавлених осіб. Для визначення можливості застосування адекватних запобіжних заходів з метою зменшення до прийнятного рівня будь-яких загроз незалежності, які є реальними чи сприймаються як такі, фахівці, за необхідності, повинні звертатися за іншими настановами до колег і керівництва, які займаються аудитом та підтвердженням довіри до ІС, а також до осіб, відповідальних за корпоративне управління.

2003 Професійна незалежність (продовження)

2.4 Неаудиторські послуги та ролі (продовження)

2.4.5 До початку надання неаудиторських послуг та виконання неаудиторських ролей фахівці з керівництвом аудиту ІС та / або особами, відповідальними за корпоративне управління, повинні, за необхідності, встановити і документально оформити розуміння:
- цілей таких неаудиторських послуг і ролей;
- характеру таких неаудиторських послуг і ролей;
- прийняття установою, що підлягає аудиту, своїх обов'язків щодо таких неаудиторських послуг і ролей;
- професійних обов'язків, пов'язаних із неаудиторськими послугами та ролями;
- будь-яких обмежень неаудиторських послуг і ролей;
- будь-яких обмежень обсягу майбутніх аудиторських послуг, які можуть надавати фахівці.

2.4.6 Якщо при виконанні завдань з аудиту та підтвердження довіри до ІС існує потенційна можливість порушення незалежності у ставленнях чи проявах внаслідок надання неаудиторських послуг та виконання неаудиторських ролей, керівництво аудиту та підтвердження довіри до ІС повинно застосувати такі запобіжні заходи, як:
- уважне відстежування проведення аудиту;
- оцінювання будь-яких значущих ознак порушення незалежності у ставленнях чи проявах внаслідок надання неаудиторських послуг і виконання неаудиторських ролей та застосування необхідних запобіжних заходів;
- інформування осіб, відповідальних за корпоративне управління, про потенційні порушення незалежності у ставленнях чи проявах і застосування запобіжних заходів.

2.5 Неаудиторські послуги та ролі, які не обмежують незалежність

2.5.1 Діяльність, яка є рутинною та адміністративною або стосується питань, які загалом є незначущими, не вважається пов'язаною з керівними обов'язками і, таким чином, не обмежує незалежність. У подальшому надання порад і рекомендацій з метою сприяння виконанню керівництвом його обов'язків не вважатиметься прийняттям на себе керівних обов'язків.

2.5.2 До неаудиторських послуг, які також не обмежують незалежність чи об'єктивність, якщо вживаються адекватні запобіжні заходи, відносяться рутинні консультації, що надають інформацію про ризики та контролі ІТ.

2.5.3 Для уникнення ризику прийняття на себе керівних обов'язків при наданні неаудиторських послуг та виконанні неаудиторських ролей у сфері, яка є або може стати об'єктом завдання з аудиту та підтвердження довіри, фахівці повинні надавати неаудиторські послуги та виконувати неаудиторські ролі тільки якщо вони переконані в тому, що керівництво виконує чи буде виконувати наступні функції, пов'язані з такими неаудиторськими послугами та ролями:
- приймати на себе усі керівні обов'язки;
- контролювати такі послуги за допомогою особи, краще – зі складу вищого виконавчого керівництва, яка має відповідні навички, знання та досвід;
- оцінювати адекватність і результати наданих послуг;
- приймати на себе відповідальність за результати послуг.

Фахівці повинні документально оформляти розгляд здатності керівництва ефективно контролювати неаудиторські послуги та ролі.

2.6 Неаудиторські послуги та ролі, які обмежують незалежність

2.6.1 Якщо фахівці приймають на себе керівні обов'язки або виконують керівну діяльність, загрози незалежності можуть стати настільки значущими, що жодні запобіжні заходи не зможуть зменшити їх до прийнятного рівня. Те, чи є діяльність керівним обов'язком, залежить від обставин і вимагає застосування професійних суджень. Приклади діяльності, яка, як правило, вважається керівним обов'язком:
- встановлення політики і стратегічного напрямку;
- керування і прийняття на себе відповідальності за дії співробітників установи;
- санкціонування операцій;
- прийняття рішень щодо того, які рекомендації повинна застосовувати функція аудиту, внутрішня функція аудиту, організація, фірма або інші треті особи;
- прийняття на себе відповідальності за розробку, застосування або забезпечення внутрішніх контролів;
- прийняття на себе відповідальності за керівництво проектом або ініціативою, пов'язаною з ІТ.

2.6.2 Вважається, що, окрім прийняття на себе керівних обов'язків, незалежність та об'єктивність обмежують наступні неаудиторські послуги та ролі:

2003 Професійна незалежність (продовження)

2.6 Неаудиторські послуги та ролі, які обмежують незалежність (продовження)

- значне залучення фахівців до контролю та роботи над плануванням, розробкою, тестуванням, встановленням, налаштуванням або функціонуванням інформаційних систем, які є суттєвими або значними щодо об'єкта перевірки завдання з аудиту та підтвердження довіри;
- розробка контролів для інформаційних систем, які є суттєвими або значними щодо об'єкта перевірки завдання з аудиту та підтвердження довіри;
- виконання ролі члена корпоративного управління, за якої фахівці несуть індивідуальну чи колективну відповідальність за прийняття керівних рішень чи затвердження політик і стандартів;
- консультування, яке є основою для рішень керівництва, або виконання керівних функцій.

2.7 Відповідність незалежності при наданні неаудиторських послуг чи виконанні неаудиторських ролей

2.7.1 Якщо це не суперечить іншим зовнішнім стандартам або законодавству, перед фахівцями не стоїть вимога бути чи задаватися незалежними при виконанні задач в рамках надання неаудиторських послуг і виконання неаудиторських ролей; проте об'єктивність залишається обов'язковою професійною вимогою. Відповідно, фахівці повинні підходити до виконання задач, що стосуються неаудиторських послуг і ролей, об'єктивно та професійно.

2.7.2 Незважаючи на те, що перед фахівцями не стоїть вимога бути незалежними при наданні неаудиторських послуг і виконанні неаудиторських ролей, фахівці повинні враховувати, чи може обмежуватися незалежність, якщо їх залучають до виконання завдань з аудиту та підтвердження довіри у значній щодо об'єкта перевірки таких завдань сфері, в якій надаються чи надавалися неаудиторські послуги та виконуються чи виконувалися неаудиторські ролі. Якщо таке потенційне порушення можливе (наприклад, якщо потім виникне необхідність у незалежному аудиті, але існує лише один фахівець, який володіє навичками, необхідними як для надання неаудиторських послуг і виконання неаудиторських ролей, так і для проведення наступного аудиту), фахівець повинен звернутися за вказівками до керівництва аудиту та, за необхідності, осіб, відповідальних за корпоративне управління, до прийняття чи надання неаудиторських послуг і виконання неаудиторських ролей.

2.7.3 При визначенні того, чи фахівець повинен надавати неаудиторські послуги та виконувати неаудиторські ролі, якщо поточні чи наступні завдання з аудиту та підтвердження довіри проводяться у сфері, в якій планується чи існує можливість надання неаудиторських послуг і виконання неаудиторських ролей самим фахівцем, необхідно отримати відповідне рішення керівництва аудиту ІС, узгоджене з особами, відповідальними за корпоративне управління. При прийнятті такого рішення керівництво аудиту ІС повинно застосовувати концептуальні основні положення. На прийняття такого рішення можуть також впливати наступні фактори:

- фахівці не повинні ставитися у таку ситуацію, коли їм доведеться перевіряти власну роботу або надавати неаудиторські послуги та виконувати неаудиторські ролі у сфері, що є значущою або значною щодо об'єкта перевірки завдань з аудиту та підтвердження довіри до ІС, до яких вони залучені чи можуть залучатися у майбутньому;
- існування доступних ресурсів для надання неаудиторських послуг і виконання функції незалежного аудиту та підтвердження довіри різними фахівцями;
- усвідомлення керівництвом та особами, відповідальними за корпоративне управління, цінності та важливості неаудиторських послуг і ролей відносно завдань з аудиту та підтвердження довіри;
- рівень ризику функції аудиту відносно неаудиторських послуг і ролей;
- вплив рішень на вимоги зовнішніх аудиторів або регулятивних органів, якщо такі існують;
- положення статуту аудиту ІС.

2.8 Прийнятність неаудиторських послуг і ролей

2.8.1 Статут аудиту ІС повинен визначати, чи дозволяється залучати фахівців до надання неаудиторських послуг і виконання неаудиторських ролей, а також загальний характер, часові рамки та обсяг таких послуг і ролей для забезпечення того, що в рамках систем, які можуть підлягати аудиту, незалежність не обмежується. Це може усунути чи мінімізувати потребу отримання конкретних розпоряджень для кожної окремої неаудиторської послуги чи ролі.

2.8.2 Фахівці повинні забезпечувати достатню впевненість у тому, що задачі, поставлені в рамках певних неаудиторських послуг і ролей, відповідають статуту аудиту. У випадку існування будь-яких відхилень їх необхідно чітко окреслити у поставлених задачах і затвердити у керівництва аудиту та підтвердження довіри до ІС та / або осіб, відповідальних за корпоративне управління.

2.8.3 Якщо статут аудиту чітко не визначає неаудиторські послуги та ролі, або якщо статуту аудиту

2003 Професійна незалежність (продовження)

2.8 Прийнятність неаудиторських послуг і ролей (продовження)

не існує, фахівці повинні звітувати керівництву аудиту та підтвердження довіри до ІС та особам, відповідальним за корпоративне управління, про характер їх залучення до надання неаудиторських послуг і виконання неаудиторських ролей. Часові рамки та обсяг залучення фахівців до надання неаудиторських послуг і виконання неаудиторських ролей повинні визначатися згідно з окремими поставленими задачами, підписуватися керівництвом функції, в рамках якої надаватимуться послуги і виконуватимуться ролі, та затверджуватися особами, відповідальними за корпоративне управління.

2.9 Звітування

2.9.1 Якщо в рамках виконання завдань з аудиту та підтвердження довіри до ІС незалежність фахівців може бути, здається чи є порушеною, але особи, відповідальні за корпоративне управління, вирішили продовжити таке завдання, звіт про таке завдання з аудиту та підтвердження довіри до ІС повинен містити інформацію, достатню для того, щоб користувачі розуміли характер потенційних порушень. Інформація, яку фахівці повинні розкрити у звіті про таке завдання з аудиту та підтвердження довіри до ІС:

- імена та посади фахівців, залучених до виконання завдань з аудиту та підтвердження довіри до ІС, незалежність яких може бути чи здаватися порушеною;
- аналіз та опис загроз незалежності;
- запобіжні заходи, застосовані для усунення чи зменшення різних загроз незалежності та об'єктивності протягом роботи над завданням та у процесі звітування;
- факт розкриття потенційного порушення незалежності особам, відповідальним за корпоративне управління, та санкціонування ними виконання чи продовження завдань з підтвердження довіри та / або неаудиторських послуг і ролей.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами
3.2 Зв'язок із процесами COBIT 5
3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA щодо аудиту та підтвердження довіри до ІС, які безпосередньо обґрунтовуються цією настановою;
- положення стандартів, які є найбільш придатні для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатні для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1001 Статут аудиту	Функція аудиту та підтвердження довіри до ІС повинна належним чином документувати у статуті аудиту функцію аудиту, зазначаючи цілі, обов'язки, повноваження та підзвітність. Функція аудиту та підтвердження довіри до ІС повинна мати статут аудиту, попередньо узгоджений і затверджений на відповідному рівні організації.
1002 Організаційна незалежність	Для забезпечення об'єктивності при виконанні завдань з аудиту та підтвердження достовірності функція аудиту та підтвердження довіри до ІС повинна бути незалежною від сфери та типу діяльності, що перевіряються.
1003 Професійна незалежність	Фахівці з аудиту та підтвердження довіри до ІС повинні бути незалежними та об'єктивними у своїх ставленнях та проявах у всіх питаннях, які стосуються виконання завдань з аудиту та підтвердження достовірності.
1005 Належна професійна ретельність	Фахівці з аудиту та підтвердження довіри до ІС повинні бути незалежними та об'єктивними у своїх ставленнях і проявах у всіх питаннях, які стосуються виконання завдань з аудиту та підтвердження достовірності. Фахівці з аудиту та підтвердження довіри до ІС повинні проявляти належну професійну ретельність, у тому числі дотримуватись діючих професійних аудиторських стандартів при плануванні, виконанні та звітуванні за результатами завдань.

2003 Професійна незалежність (продовження)

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
• процеси COBIT 5;
• призначення процесів COBIT 5.
Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.
MEA03 Відстежувати, оцінювати та аналізувати відповідність зовнішнім вимогам	Забезпечити дотримання організацією діючих зовнішніх вимог.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
• у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
• у керівництва;
• в органах корпоративного управління організацією, наприклад,в аудиторському комітеті.

4. Термінологія

Термін	Визначення
Незалежність	Свобода від обставин, що загрожують об'єктивності чи створюють враження об'єктивності. Необхідно, щоб такі загрози об'єктивності нейтралізувалися на рівні окремого аудитора, завдання і на функціональному та організаційному рівнях. Незалежність включає в себе незалежність у поглядах і незалежність у проявах.
Незалежність у поглядах	Стан мислення, що дозволяє робити висновки, не зазнаючи жодних впливів, які можуть скомпрометувати професійні судження, дозволяючи фахівцю діяти цілісно та проявляти об'єктивність і професійний скептицизм.
Незалежність у проявах	Ухиляння від фактів та обставин, які є настільки значущими, що розсудлива інформована третя особа, зваживши усі підтверджуючі конкретні факти та обставини, може дійти до висновку про компрометацію цілісності, об'єктивності чи професійного скептицизму аудиторів або члена аудиторської групи.
Об'єктивність	Здатність неупереджено висловлювати судження, робити висновки та давати рекомендації.
Порушення	Умови, які викликають погіршення або за яких послаблюється здатність досягати цілей аудиту. Порушення організаційної незалежності та індивідуальної об'єктивності може виникати внаслідок особистого конфлікту інтересів, обмеження обсягів, обмеження доступу до документів, персоналу, обладнання чи майна та обмеження ресурсів (таких як фінансування або кадрове забезпечення).
Професійний скептицизм	Ставлення, яке включає допитливе мислення та критичну оцінку аудиторських доказів. Джерело: AU 230.07, AICPA.
Професійні судження	Застосування відповідних знань і досвіду при інформованому прийнятті рішень про напрямки дій, що відповідають обставинам завдань з аудиту та підтвердження довіри до ІС.

2003 Професійна незалежність (продовження)

4. Термінологія (продовження)

Термін	Визначення
Суттєвість	Аудиторська концепція важливості елемента інформації, враховуючи її вплив чи наслідки на функціонування об'єкта перевірки в цілому. Вираження відносної значущості чи важливості окремого питання в контексті організації в цілому.
Цілісність	Захист інформації від неналежної зміни чи знищення, у тому числі забезпечення автентичності та незаперечності інформації.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2004 Обґрунтовані очікування

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1. Мету настанови
1.2. Зв'язок зі стандартами
1.3. Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови полягає у сприянні застосуванню фахівцями з аудиту та підтвердження довіри до ІС настанови обґрунтованих очікувань при виконанні завдань з аудиту. Основні характеристики, щодо яких фахівці повинні мати обґрунтовані очікування:
- завдання з аудиту можуть виконуватися у відповідності до цих стандартів або інших діючих стандартів та нормативних документів і повинні завершитися формуванням професійної думки чи висновків;
- обсяг завдань з аудиту дає можливість висловити професійну думку чи висновки щодо об'єкта перевірки;
- керівництво надає фахівцям доречну, відповідну та своєчасну інформацію, необхідну для виконання завдань з аудиту.

1.1.2 Окрім того, ця настанова сприяє розгляду фахівцями з аудиту та підтвердження довіри до ІС обмежень обсягу робіт і надає вказівки щодо прийняття змін в умовах.

1.1.3 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1001 Статут аудиту
1.2.2 Стандарт 1004 Обґрунтовані очікування

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані із завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Стандарти і нормативні документи
2.2 Обсяг
2.3 Обмеження обсягу
2.4 Інформація
2.5 Прийняття змін в умовах завдань

2.1 Стандарти і нормативні документи

2.1.1 Статут аудиту визначає стандарти, яких повинні дотримуватися функція аудиту і фахівці згідно зі Стандартом 1001«Статут аудиту».

2.1.2 До початку виконання завдань з аудиту фахівці повинні зібрати та оцінити усі відповідні нормативні документи і стандарти, перелічені у статуті аудиту, і звертатися до них протягом виконання завдань, щоб визначити, чи є у них обґрунтовані очікування щодо можливості завершення завдань з аудиту у відповідності до цих стандартів і нормативних документів, і чи завершаться завдання з аудиту формуванням професійної думки чи висновків.

2.1.3 Якщо фахівці визначають неможливість виконання завдань з аудиту у відповідності до одного чи кількох відповідних діючих стандартів і нормативних документів і, відповідно, формування професійної думки чи висновків, вони повинні:
- повідомити керівництво аудиту та підтвердження довіри до ІС і осіб, відповідальних за корпоративне управління, про виявлені проблеми відповідності стандартам і нормативним

2004 Обґрунтовані очікування (продовження)

2.1 Стандарти і нормативні документи (продовження)

документам;
- запропонувати зміну в умовах завдань або повідомити про неприйняття запропонованих завдань.

2.2 Обсяг

2.2.1 До того, як взятися за завдання з аудиту, фахівці повинні оцінити їх обсяг. Вони повинні визначити, чи обсяг аудиту чітко задокументований, і чи дозволяє він сформувати професійну думку чи висновки щодо об'єкта перевірки.

2.2.2 Обсяг завдань з аудиту повинен бути чітко задокументованим, щоб унеможливити різні тлумачення сфер обсягу завдань (наприклад, процесів, видів діяльності, систем). Занадто нечітко описаний обсяг не дозволить фахівцям сформувати свою професійну думку чи висновки, оскільки він не дає впевненості у тому, що оцінено всі сфери обсягу.

2.2.3 Якщо фахівці визначають, що обсяг завдань з аудиту не дозволяє їм сформувати свою професійну думку чи висновки, вони повинні:
- повідомити керівництво аудиту та підтвердження довіри до ІС і осіб, відповідальних за корпоративне управління, про виявлені проблеми з обсягом;
- запропонувати зміну в умовах завдань або повідомити про неприйняття запропонованих завдань з аудиту.

2.3 Обмеження обсягу

2.3.1 Певні обмеження обсягу можуть мати місце до початку або протягом виконання завдань з аудиту. На такі обмеження обсягу можуть впливати різні фактори, як, наприклад:
- доречна, відповідна та своєчасна інформація, необхідна для виконання завдань з аудиту, недоступна;
- (основна) організація, що підлягає аудиту, недоступна;
- зазначені часові рамки недостатні для виконання завдань з аудиту в повному обсязі;
- керівництво намагається обмежити обсяг завдань з аудиту до окремих сфер;
- обсяг завдань з аудиту занадто малий або занадто великий для формування висновків щодо об'єкта перевірки;
- рівень децентралізації ускладнює формування висновків щодо комплексності об'єкта перевірки;
- наявність достатньої кількості фахівців, які володіють відповідними навичками для виконання завдання з аудиту в поточному обсязі;
- структура звітування функції аудиту, наприклад, якщо функція аудиту не звітує відповідному рівню керівництва в організації, вона може бути направлена на оцінювання не всіх елементів обсягу.

2.3.2 Фахівці повинні враховувати, чи такі обмеження обсягу все ж надають обґрунтовані очікування щодо того, що завдання з аудиту завершаться формуванням професійної думки чи висновків. Якщо вони визначають, що ця умова не буде дотримана, вони не повинні приймати такі завдання.

2.3.3 Якщо фахівці приходять до висновку, що вони все ж мають обґрунтовані очікування стосовно того, що, незважаючи на обмеження обсягу, завдання завершаться формуванням професійної думки чи висновків, вони повинні прийняти або продовжити виконання таких завдань з аудиту. Обмеження обсягу необхідно чітко описувати у звіті щодо завдань з аудиту та підтвердження довіри до ІС.

2.4 Інформація

2.4.1 Згідно зі Стандартом 1001«Статут аудиту» статут аудиту визначає право доступу до інформації, систем, персоналу та приміщень організації, пов'язане з виконанням завдань з аудиту.

2.4.2 До прийняття завдань з аудиту, фахівці повинні визначити і розглянути будь-які обмеження, пов'язані з правом доступу до доречної, відповідної та своєчасної інформації в рамках виконання завдань з аудиту. Вони повинні мати обґрунтовані очікування щодо того, що таке право доступу відповідає умовам статуту аудиту, або що потенційні відхилення від них можуть запобігати формуванню фахівцями їх професійної думки чи висновків щодо об'єкта перевірки.

2.4.3 Виконання завдань з аудиту та підтвердження довіри може вимагати від адміністративного та вищого виконавчого керівництва здійснення діяльності, пов'язаної з оцінюванням. До початку виконання завдань з аудиту необхідно оцінювати можливість настання такої події, а також потребу оцінювання фахівцями таких осіб або відповідної інформації. До

2004 Обґрунтовані очікування (продовження)

2.4 Інформація (продовження)

початку виконання завдань з аудиту може бути необхідним застосування у тому числі таких пом'якшуючих дій, як:
- забезпечення того, що статут аудиту надає функції аудиту і фахівцям відповідні повноваження;
- отримання у письмовій формі чіткої підтримки від осіб, відповідальних за корпоративне управління, наприклад, від ради директорів та аудиторського комітету;
- участь членів ради та вищого виконавчого керівництва, якщо необхідний доступ до адміністративного та вищого виконавчого керівництва.

2.4.4 Якщо фахівці роблять висновок, що право доступу до інформації не дозволяє їм сформувати свою професійну думку чи висновки, вони повинні:
- повідомити керівництво аудиту та підтвердження довіри до ІС і осіб, відповідальних за корпоративне управління, про виявлені проблеми з правом доступу до доречної, відповідної та своєчасної інформації;
- запропонувати зміну в умовах завдань або повідомити про неприйняття запропонованих завдань з аудиту.

2.5 Прийняття змін в умовах завдань

2.5.1 Фахівці не повинні приймати зміни в умовах завдань з аудиту, якщо згідно з їхніми професійними судженнями це не виправдовується обставинами.

2.5.2 Якщо до завершення виконання завдань з аудиту фахівцям пропонують прийняти такі зміни в умовах, які знижують рівень впевненості, вони повинні визначити за допомогою своїх професійних суджень, чи це виправдовується обставинами.

2.5.3 У випадку змін в умовах завдань з аудиту такі зміни повинні бути зафіксовані у письмовій формі та затверджені як фахівцями, так і керівництвом аудиту та підтвердження довіри до ІС. Після завершення виконання завдань з аудиту такі зміни в умовах повинні бути чітко зазначені у звіті про результати завдань з аудиту та підтвердження довіри.

2.5.4 Якщо фахівці не приймають зміни в умовах завдань з аудиту, і керівництво не дозволяє їм продовжити виконання таких завдань, фахівці, проконсультувавшись з керівництвом аудиту та підтвердження достовірності,повинні:
- припинити виконання завдань з аудиту;
- визначити за допомогою своїх професійних суджень, чи існує необхідність звітувати про такі обставини особам, відповідальним за корпоративне управління, раді директорів чи навіть регуляторним органам.

3. Зв'язок зі стандартами і процесами COBIT 5

Цей розділ розглядає такі придатні питання, як:

3.1 Зв'язок зі стандартами

3.2 Зв'язок із процесами COBIT 5

3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:
- найбільш придатні стандарти ISACA, які безпосередньо обґрунтовуються цією настановою;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1001 Статут аудиту	Функція аудиту та підтвердження довіри до ІС повинна належним чином документувати у статуті аудиту функцію аудиту, зазначаючи цілі, обов'язки, повноваження та підзвітність. Функція аудиту та підтвердження довіри до ІС повинна мати статут аудиту, попередньо узгоджений і затверджений на відповідному рівні організації.

2004 Обґрунтовані очікування (продовження)

3.1 Зв'язок зі стандартами (продовження)

Назва стандарту	Відповідні положення стандарту
1004 Обґрунтовані очікування	Фахівці з аудиту та підтвердження довіри до ІС повинні мати обґрунтовані очікування щодо виконання завдань згідно зі стандартами аудиту та підтвердження довіри до ІС і, за необхідності, іншими відповідними професійними чи галузевими стандартами та діючими нормами, щоб у результаті висловити свою професійну думку чи висновок. Фахівці з аудиту та підтвердження довіри до ІС повинні мати обґрунтовані очікування щодо обсягу завдань, який має бути таким, щоб забезпечити надання висновку про об'єкт перевірки та вирішити питання, пов'язані з будь-якими обмеженнями. Фахівці з аудиту та підтвердження довіри до ІС повинні мати обґрунтовані очікування щодо усвідомлення керівництвом своїх обов'язків та відповідальності, пов'язаних із забезпеченням своєчасною та відповідною інформацією, необхідною для виконання поставлених завдань.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
• Процеси COBIT 5
• Призначення процесів COBIT 5
Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Назва і номер процесу COBIT 5	Мета процесу
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.
MEA03 Відстежувати, оцінювати та аналізувати відповідність зовнішнім вимогам.	Забезпечити дотримання організацією діючих зовнішніх вимог.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
• у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
• у керівництва;
• в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
• в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
(немає)	

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2005 Належна професійна ретельність

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови полягає у роз'ясненні терміну «належна професійна ретельність» та його застосуванні при цілісному та ретельному виконанні завдань з аудиту згідно з Кодексом професійної етики ISACA.

1.1.2 Ця настанова пояснює, як фахівці з аудиту та підтвердження довіри до ІС повинні застосовувати належну професійну ретельність при плануванні, виконанні та звітуванні за результатами завдань з аудиту.

1.1.3 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1	Стандарт 1002	Організаційна незалежність
1.2.2	Стандарт 1003	Професійна незалежність
1.2.3	Стандарт 1005	Належна професійна ретельність
1.2.4	Стандарт 1006	Професійність
1.2.5	Стандарт 1205	Докази

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані із завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Професійний скептицизм і компетенція
2.2 Застосування
2.3 Цикл завдань
2.4 Інформування
2.5 Управління інформацією

2.1 Професійний скептицизм і компетенція

2.1.1 Належна професійна ретельність відноситься до застосування професійних суджень при проведенні роботи. Належна професійна ретельність означає, що фахівці повинні підходити до питань, які вимагають застосування професійних суджень з професійним скептицизмом, старанністю, цілісністю та ретельністю. Вони повинні дотримуватися такого відношення протягом виконання всіх завдань.

2.1.2 Фахівці повинні бути компетентними, незалежними та об'єктивними у всіх питаннях, пов'язаних із виконанням завдань з аудиту. Вони повинні бути чесними, справедливими та неупередженими при розгляді проблем і формуванні висновків.

2.1.3 Фахівці, що застосовують належну професійну ретельність, повинні враховувати можливість існування неефективності, неправильного застосування, помилок і винятків, некомпетентності, конфліктів інтересів і шахрайства. Окрім того, фахівці повинні бути уважними до певних видів діяльності або обставин, за яких виникають такі проблеми.

2.1.4 Постійно знайомлячись із нововведеннями у сфері професійних стандартів і дотримуючись їх, фахівці демонструють достатній рівень розуміння та професійної компетенції для досягнення цілей аудиту та підтвердження довіри до ІС. Детальні вказівки наведено у Стандарті 1006

2005 Належна професійна ретельність (продовження)

2.1 Професійний скептицизм і компетенція (продовження)		«Професійність».
	2.1.5	Фахівці повинні старанно виконувати завдання з аудиту, дотримуючись професійних стандартів та законодавчих і регулятивних вимог.
2.2 Застосування	2.2.1	Належна професійна ретельність повинна розповсюджуватися на кожен аспект аудиту, включаючи, але не обмежуючись оцінюванням ризиків аудиту, прийняттям завдань з аудиту, встановленням обсягу, формулюванням цілей, плануванням і проведенням аудиту, розподілом ресурсів, вибором аудиторських тестів, оцінюванням результатів тестів, документальним оформленням аудиту, формуванням аудиторських висновків, звітуванням і досягненням аудиторських результатів. Таким чином, фахівці повинні визначати або оцінювати: • тип, рівень, навички та компетенцію ресурсів, необхідних для досягнення цілей аудиту та підтвердження довіри до ІС; • значущість виявлених ризиків та їх потенційний вплив на об'єкт аудиту; • достатність, обґрунтованість та відповідність зібраних аудиторських доказів; • компетенцію, цілісність і висновки інших осіб, на роботу яких покладаються фахівці.
	2.2.2	Належна професійна ретельність також вимагає, щоб фахівці виконували усі завдання, враховуючи концепцію достатньої впевненості.
	2.2.3	Фахівці повинні сумлінно працювати у рамках закону в інтересах зацікавлених сторін, дотримуючись високих стандартів поведінки та репутації, не дискредитуючи свою професію.
2.3 Цикл завдань	2.3.1	Для забезпечення доступності відповідних ресурсів і своєчасного виконання завдань з аудиту фахівці повинні планувати завдання з аудиту повністю і своєчасно, застосовуючи належну професійну ретельність. Для виконання завдань з аудиту фахівці, залучені до роботи над проектом, повинні колективно володіти необхідними навичками, знаннями та відповідною компетенцією .
	2.3.2	Фахівці повинні виконувати завдання з аудиту, застосовуючи належну професійну ретельність, тобто дотримуючись відповідних професійних стандартів з метою забезпечення довіри і повноти професійних суджень та аудиторських висновків.
2.4 Інформування	2.4.1	До початку проекту необхідно проінформувати членів групи про визначені ролі та обов'язки, щоб забезпечити дотримання групою відповідних професійних стандартів під час виконання завдань з аудиту.
	2.4.2	Під час виконання завдань з аудиту фахівці повинні забезпечити належне інформування організації, що підлягає аудиту, та відповідних зацікавлених сторін з метою налагодження співпраці з ними.
	2.4.3	Фахівці повинні відправляти отримані дані щодо завдань з аудиту на розгляд організації, що підлягає аудиту.
	2.4.4	Фахівці повинні документально оформляти та звітувати відповідним сторонам про ускладнення, пов'язані із застосуванням професійних стандартів, з метою вирішення таких ускладнень.
	2.4.5	Фахівці повинні застосовувати належну професійну ретельність при інформуванні відповідних сторін про результати виконаної роботи.
2.5 Отримання та управління інформацією	2.5.1	Фахівці повинні мати обґрунтовані очікування щодо розуміння керівництвом своїх обов'язків та відповідальності при наданні доречної, відповідної та своєчасної інформації, необхідної для виконання завдань з аудиту.
	2.5.2	Фахівці повинні вживати необхідні заходи для збереження комерційних таємниць та конфіденційної інформації, отриманої в рамках виконання своїх обов'язків, окрім випадків, коли це вимагається законом.
	2.5.3	Інформація повинна зберігатися і бути знищеною належним чином згідно з політикою організації та відповідними законами, нормами і правилами.

3. Зв'язок зі стандартами і процесами COBIT 5

2005 Належна професійна ретельність (продовження)

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами
3.2 Зв'язок із процесами COBIT 5
3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA, які безпосередньо обґрунтовуються цією настановою;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1002 Організаційна незалежність	Для забезпечення об'єктивності при виконанні завдань з аудиту та підтвердження достовірності функція аудиту та підтвердження довіри до ІС повинна бути незалежною від сфери та типу діяльності, що перевіряються.
1003 Професійна незалежність	Фахівці з аудиту та підтвердження довіри до ІС повинні бути незалежними та об'єктивними у своїх ставленнях і проявах у всіх питаннях, які стосуються виконання завдань з аудиту та підтвердження довіри.
1005 Належна професійна ретельність	Фахівці з аудиту та підтвердження довіри до ІС повинні проявляти належну професійну ретельність, у тому числі дотримуватись діючих професійних стандартів аудиту при плануванні, виконанні та звітуванні за результатами завдань.
1006 Професійність	Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні колективно володіти необхідними навичками і проявляти професійність при виконанні завдань з аудиту та підтвердження довіри до ІС, а також бути професійно компетентними для здійснення роботи. Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні мати достатні знання про об'єкт перевірки. Фахівці з аудиту та підтвердження довіри до ІС повинні підтримувати свою професійну компетенцію, здобуваючи додаткову професійну освіту та підготовку.
1205 Аудиторські докази	Фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази, щоб зробити обґрунтовані висновки, на які спиратимуться результати завдань. Фахівці з аудиту та підтвердження довіри до ІС повинні оцінювати достатність отриманих доказів для обґрунтування висновків та досягнення цілей завдань.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:

- Процеси COBIT 5
- Цілі процесів COBIT 5

Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Process Purpose
EDM01 Забезпечувати впровадження та підтримку основних положень корпоративного управління	Забезпечити єдиний підхід, інтегрований та узгоджений з підходом організації до корпоративного управління. Приймати такі рішення у сфері IT, які відповідатимуть стратегіям і цілям організації. Здійснювати ефективний і прозорий нагляд за процесами, пов'язаними з IT, та підтверджувати їх відповідність законодавчим і регулятивним вимогам, а також забезпечити дотримання членами керівної ради вимог до корпоративного управління.
APO07 Управляти персоналом	Оптимізувати можливості персоналу таким чином, щоб вони відповідали цілям організації.

2005 Належна професійна ретельність (продовження)

3.2 Зв'язок із процесами COBIT 5 (продовження)

Процес COBIT 5	Process Purpose
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.
MEA03 Відстежувати, оцінювати та аналізувати відповідність зовнішнім вимогам.	Забезпечити дотримання організацією діючих зовнішніх вимог.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:

- у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- в інших настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Професійна компетенція	Підтверджений рівень здатності, разом з професійним досвідом, який часто пов'язують із кваліфікаціями, що призначаються відповідними професійними органами, та відповідністю їх нормам практики та стандартам.
Професійний скептицизм	Ставлення, яке включає допитливе мислення та критичну оцінку аудиторських доказів. Джерело: AU 230.07, AICPA.
Професійні судження	Застосування відповідних знань і досвіду при інформованому прийнятті рішень про напрямки дій, що відповідають обставинам завдань з аудиту та підтвердження довіри до ІС.

5. Дата набуття чинності

5.1 Дата набуття чинності

Цей переглянутий принцип є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2006 Професійність

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Ця настанова надає вказівки, які сприяють фахівцям з аудиту та підтвердження довіри до ІС у набутті необхідних навичок і знань та підтриманні професійної компетенції при виконанні завдань з аудиту.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1005 Належна професійна ретельність
1.2.2 Стандарт 1006 Професійність
1.2.3 Стандарт 1201 Планування завдань
1.2.4 Стандарт 1203 Ефективність і нагляд

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані із завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Професійна компетенція
2.2 Оцінювання
2.3 Досягнення необхідного рівня компетенції

2.1 Професійна компетенція

2.1.1 Професійна компетенція означає володіння навичками, знаннями та компетентністю, що ґрунтуються на відповідному рівні освіти та досвіді, для належного виконання завдань з аудиту.

2.1.2 Враховуючи відповідні цільові орієнтири, керівництво аудиту та підтвердження довіри до ІС повинно надати інформацію про бажаний та / або очікуваний рівень професійної компетенції для виконання різних ролей при виконанні завдань з аудиту, а також забезпечити періодичну перевірку та оновлення таких цільових орієнтирів. Керівництво аудиту та підтвердження довіри до ІС повинно документально оформляти професійну компетенцію, необхідну для виконання роботи на різних рівнях, наприклад, розробити матрицю навичок, яка описує професійну компетенцію, необхідну для виконання роботи на різних рівнях.

2.1.3 Керівництво аудиту та підтвердження довіри до ІС повинно забезпечити достатню впевненість у наявності визначених у плані аудиту ІС компетентних ресурсів, необхідних для виконання завдань з аудиту. Необхідно підтвердити та забезпечити наявність таких компетентних ресурсів до початку виконання завдань.

2.1.4 Керівництво аудиту та підтвердження довіри до ІС несе відповідальність за забезпечення компетентності членів групи для виконання завдань з аудиту. Визначення основних професійних компетенцій членів групи сприятиме ефективному використанню доступних ресурсів.

2.1.5 Фахівці повинні забезпечити достатню впевненість у тому, що вони володіють необхідним рівнем професійної компетенції. Фахівці повинні нести відповідальність за набуття необхідних професійних і технічних навичок і знань для виконання будь-якого завдання, яке вони погоджуються виконувати.

2.1.6 Необхідні навички і знання можуть різнитися залежно від посади та ролі фахівців у рамках

2006 Професійність (продовження)

2.1 Професійна компетенція (продовження)		виконання завдань з аудиту. Вимоги до навичок і знань керівництва повинні відповідати рівню їхньої відповідальності.
	2.1.7	При визначенні та управлінні ризиками та контролями навички та знання охоплюють професійність, а також аудиторській інструментарій і методики. Фахівці повинні володіти аналітичними і технічними знаннями та навичками опитування, міжособистого спілкування та подачі матеріалу.
	2.1.8	Фахівці повинні володіти знаннями, необхідними для виявлення, визначення впливу та звітування про можливі обставини чи відхилення, які є суттєвими для завдань з аудиту.
	2.1.9	Фахівці повинні вміти впізнавати можливі ознаки шахрайства.
	2.1.10	Фахівці повинні мати загальні знання про основи бізнесу, наприклад, про економіку, фінанси, бухгалтерську справу, інформаційні технології, ризики, податки та закони, щоб не пропустити жодне потенційне питання чи недолік.
	2.1.11	Необхідно, щоб фахівці ділилися з членами групи власним досвідом, засвоєним передовим досвідом, отриманими уроками та набутими знаннями з метою вдосконалення професійної компетенції ресурсів. Окрім того, професійні компетенції членів групи вдосконалюються за допомогою участі у заходах по формуванню колективу, робочих групах, конференціях, семінарах, лекціях, а також інших типів взаємодії.
	2.1.12	Для забезпечення придбання відповідних навичок необхідно оцінювати альтернативні способи отримання таких навичок, включаючи залучення певних ресурсів на підрядній основі, передачу підрядникам частини задач з аудиту та підтвердження довіри до ІС та / або відстрочування виконання завдань з аудиту до появи необхідних навичок.
	2.1.13	Зовнішні знання можна отримати шляхом передачі частини завдань підрядникам. Співпраця залучених ресурсів із внутрішніми фахівцями також забезпечує розвиток та підтримання знань і навичок внутрішніх ресурсів.
	2.1.14	У випадку передачі будь-якої частини завдань з аудиту підряднику або отримання допомоги експертів необхідно забезпечити достатню впевненість у тому, що залучена організація або зовнішні експерти володіють необхідною професійною компетенцією.
	2.1.15	У випадку отримання допомоги експертів на постійній основі необхідно періодично оцінювати, контролювати і переглядати професійну компетенцію таких зовнішніх експертів відносно професійних стандартів чи цільових орієнтирів.
2.2 Оцінювання	2.2.1	Фахівці повинні постійно контролювати свої навички та знання для підтримання необхідного рівня професійної компетенції. Керівництво аудиту та підтвердження довіри до ІС повинно періодично оцінювати професійну компетенцію.
	2.2.2	Оцінювання діяльності фахівців повинне здійснюватися справедливо, прозоро, загально зрозуміло, однозначно, без упереджень і з врахуванням загальноприйнятої практики у відповідному робочому середовищі.
	2.2.3	Необхідно чітко визначати критерії оцінювання і процедури, але вони можуть різнитися залежно від таких обставин, як географічне положення, політичний клімат, характер завдань, культура тощо.
	2.2.4	У випадку групи фахівців оцінювання повинне виконуватися внутрішньо між групами чи окремими особами на міжфункціональній основі.
	2.2.5	У випадку окремого (єдиного) незалежного фахівця оцінювання повинне, по можливості, виконуватися експертом. Якщо проведення зовнішнього контролю неможливе, необхідно здійснити та документально оформити самооцінювання.
	2.2.6	Оцінювання діяльності фахівців повинне здійснюватися керівництвом відповідного рівня.
	2.2.7	Необхідно належним чином розглядати розбіжності, помічені при проведенні оцінювання.
2.3 Досягнення необхідного рівня компетенції	2.3.1	Помічені розбіжності між наявним і очікуваним рівнем професійної компетенції повинні письмово фіксуватися та аналізуватися. У випадку значущих порушень будь-яким ресурсом такий ресурс не повинен залучатися до виконання завдань з аудиту.
	2.3.2	Важливо встановлювати причини розбіжностей і якнайшвидше вживати відповідні корегуючи заходи, такі як підготовка та додаткова професійна освіта (ДПО).
	2.3.3	Підготовка, необхідна для виконання завдань з аудиту, повинна виконуватися в обґрунтовані часові рамки до початку аудиторської діяльності.
	2.3.4	Ефективність підготовки повинна оцінюватися після її завершення в обґрунтовані часові рамки.
	2.3.5	Документальне оформлення необхідних навичок, як, наприклад, розробка керівництвом

2006 Професійність (продовження)

2.3 Досягнення необхідного рівня компетенції (продовження)

аудиту та підтвердження довіри до ІС матриці навичок (пункт 2.1.2), сприятиме визначенню розбіжностей і потреб у підготовці. Така матриця може посилатися на наявні ресурси та їхні навички і знання.

2.3.6 Необхідно зберігати та аналізувати, а також при майбутньому використанні посилатися на документи про здійснену підготовку та відгуки про неї та її ефективність.

2.3.7 ДПО – це методика, прийнята для підтримання професійної компетенції та оновлення навичок і знань. Фахівці повинні слідувати вимогам політик щодо ДПО, встановлених відповідними професійними органами, з якими вони пов'язані.

2.3.8 Програми ДПО повинні сприяти вдосконаленню навичок і знань та відповідати професійним і технічним вимогам підтвердження довіри, безпеки та управління ІС. Як правило, професійні органи рекомендують програми, що сприяють визнанню ДПО. Фахівці повинні дотримуватися норм, рекомендованих відповідними професійними органами.

2.3.9 Як правило, професійні органи рекомендують методику отримання залікових одиниць ДПО і встановлюють мінімальну кількість залікових одиниць, яку необхідно періодично отримувати, по складових. Фахівці повинні дотримуватися норм, рекомендованих відповідними професійними органами. Якщо фахівці пов'язані з кількома професійними органами, для отримання мінімальної кількості залікових одиниць вони можуть застосовувати свої професійні судження, щоб здобути певну користь від залікових одиниць ДПО, отриманих в рамках відповідних програм за умови дотримання правил / настанов таких професійних органів.

2.3.10 ISACA має детальну політику щодо ДПО, яка застосовується до її членів і власників сертифікату CISA. Фахівці, що є власниками сертифікату CISA, повинні слідувати політиці ISACA щодо ДПО. Детальнішу інформацію про цю політику можна знайти за наступним посиланням: www.isaca.org/CISAcpepolicy.

2.3.11 Згідно з рекомендаціями відповідних професійних органів, у тому числі ISACA, фахівці повинні вести записи по програмах ДПО, зберігати їх протягом певного періоду часу і, за необхідності, надавати їх для аудиту.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами

3.2 Зв'язок із процесами COBIT 5

3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA, які безпосередньо обґрунтовуються цією настановою;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1005 Належна професійна ретельність	Фахівці з аудиту та підтвердження довіри до ІС повинні проявляти належну професійну ретельність, у тому числі дотримуватись діючих професійних аудиторських стандартів при плануванні, виконанні та звітуванні за результатами завдань.
1006 Професійність	Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні колективно володіти необхідними навичками і проявляти професійність при виконанні завдань з аудиту та підтвердження довіри до ІС, а також бути професійно компетентними для здійснення роботи. Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні мати достатні знання про об'єкт перевірки. Фахівці з аудиту та підтвердження довіри до ІС повинні підтримувати свою професійну компетенцію, здобуваючи додаткову професійну освіту та підготовку.

2006 Професійність (продовження)

3.1 Зв'язок зі стандартами (продовження)

Назва стандарту	Відповідні положення стандарту
1201 Планування завдань	Фахівці з аудиту та підтвердження довіри до ІС повинні планувати кожне завдання з аудиту та підтвердження довіри до ІС таким чином, щоб воно відповідало: • цілі (цілям), обсягу, часовим рамкам і запланованим результатам; • діючим законам і професійним аудиторським стандартам; • застосуванню, за необхідності, ризик-орієнтованого підходу; • питанням, що виникають у зв'язку зі специфікою завдань; • вимогам до документації та звітності. Фахівці з аудиту та підтвердження довіри до ІС повинні розробляти та документально оформляти проектний план завдань з аудиту та підтвердження довіри до ІС, що описує: • характер, цілі та часові рамки завдань, а також потреби у ресурсах; • терміни проведення та обсяг аудиторських процедур, необхідних для виконання завдань.
1203 Ефективність і нагляд	Фахівці з аудиту та підтвердження довіри до ІС повинні забезпечити контроль за роботою аудиторського персоналу, яку вони курують, щоб досягти аудиторських цілей у відповідності до діючих професійних аудиторських стандартів. Фахівці з аудиту та підтвердження довіри до ІС повинні братися за виконання тільки таких задач, які можна завершити за допомогою уже наявних знань і навичок, або якщо вони мають обґрунтовані очікування щодо набуття таких навичок у процесі роботи чи виконання задач під наглядом.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
• Процеси COBIT 5
• Цілі процесів COBIT 5
Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
EDM04 Забезпечувати оптимізацію ресурсів	Забезпечити оптимальне задоволення потреб організації в ресурсах, оптимізацію витрат, пов'язаних з IT, а також збільшення ймовірності отримання вигід / переваг і збільшення готовності до майбутніх змін.
APO07 Управляти персоналом	Оптимізувати можливості персоналу таким чином, щоб вони відповідали цілям організації.
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
• у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
• у керівництва;
• в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
• в інших настановах (наприклад, у книгах, документах чи інших настановах).

2006 Професійність (продовження)

4. Термінологія

Термін	Визначення
Професійна компетенція	Підтверджений рівень здатності, разом з професійним досвідом, який часто пов'язують із кваліфікаціями, що призначаються відповідними професійними органами, та відповідністю їх нормам практики та стандартам.
Професійність	Володіння навичками та досвідом.
Професійні судження	Застосування відповідних знань і досвіду при інформованому прийнятті рішень про напрямки дій, що відповідають обставинам завдань з аудиту та підтвердження довіри до ІС.
Суттєвість	Аудиторська концепція важливості елемента інформації, враховуючи її вплив чи наслідки на функціонування об'єкта перевірки в цілому. Вираження відносної значущості чи важливості окремого питання в контексті організації в цілому.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2007 Твердження

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови полягає у детальному описі різних тверджень, управлінні фахівцями з аудиту та підтвердження довіри до ІС при підтвердженні того, що критерії, за якими здійснюватиметься оцінювання об'єкта перевірки, відповідають твердженням, а також у наданні вказівок щодо формулювання висновків та підготовки звітів щодо тверджень.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1007 Твердження
1.2.2 Стандарт 1008 Критерії
1.2.3 Стандарт 1204 Суттєвість
1.2.4 Стандарт 1206 Залучення інших експертів
1.2.5 Стандарт 1401 Звітування

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані із завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Твердження
2.2 Об'єкт перевірки та критерії
2.3 Твердження, зроблені третіми особами
2.4 Висновки та звіти

2.1 Твердження

2.1.1 Твердження – це будь-яке офіційне висловлювання чи група висловлювань щодо того, чи об'єкт перевірки базується на або відповідає обраним критеріям. Фахівці повинні розглядати твердження протягом виконання завдань з аудиту, підтверджувати їх отримання та відображати це у своїх аудиторських звітах.

2.1.2 Можуть розглядатися такі прості твердження, як:
- **конфіденційність** (збереження встановлених обмежень на доступ до та розкриття інформації, у тому числі засобів захисту комерційних таємниць та конфіденційної інформації);
- **повнота** (фіксування всієї діяльності, інформації та інших даних, які повинні записуватися, наприклад, відображення всіх змін системи ІТ, які вводяться в дію, у програмі стеження за управлінням змінами);
- **точність** (належний запис сум, дат та інших даних, пов'язаних з діяльністю, що фіксується, наприклад,належне відображення даних, пов'язаних із введенням в дію змін системи ІТ, у записах про зміни у програмі стеження за управлінням змінами);
- **цілісність** (отримання інформації, доказів та інших даних із достовірних і надійних джерел, наприклад, записи про зміни, необхідні фахівцям, надаються менеджером із забезпечення відповідності, який є достовірним і надійним джерелом в організації);
- **наявність** (існування та доступність інформації, доказів та інших даних, необхідних для виконання завдань з аудиту, наприклад, існування та легкодоступність необхідних записів про

2007 Твердження (продовження)

2.1 Твердження (продовження)

зміни у програмі стеження за управлінням змінами);
- **відповідність** (фіксування інформації, доказів та інших даних згідно з вимогами організації та нормативними або іншими відповідними вимогами, наприклад, наявність необхідних полів у записах про зміни у програмі стеження за управлінням змінами згідно з відповідними вимогами).

2.1.3
- Керівництво несе відповідальність за визначення та затвердження об'єкта перевірки та відповідних тверджень. Фахівці повинні забезпечити відповідність тверджень, зроблених керівництвом, очікуванням обізнаного читача чи користувача у порівнянні з положеннями інших стандартів.

2.1.4
- Передумовою прийняття фахівцями завдань з аудиту повинно бути підтвердження керівництвом повного розуміння своїх обов'язків, пов'язаних із наданням фахівцям всієї необхідної інформації щодо об'єкта перевірки та тверджень. Якщо фахівці вважають, що керівництво не зможе виконати такі обов'язки, вони повинні:
- повідомити керівництво аудиту та підтвердження довіри до ІС та осіб, відповідальних за корпоративне управління, про виявлену проблему;
- не приймати запропоновані завдання з аудиту.

2.1.5
- Фахівці повинні переглядати твердження, обрані для виконання завдань з аудиту, та забезпечити їх:
- **достатність** (достатню кількість для досягнення цілей завдань з аудиту, пов'язаних із висловленням професійних суджень чи висновків щодо об'єкта перевірки в цілому);
- **обґрунтованість** (можливість здійснювати перевірку, розглядаючи об'єкт перевірки в цілому);
- **відповідність** (прямий зв'язок з об'єктом в цілому та сприяння досягненню цілей завдань з аудиту).

2.2 Об'єкт перевірки та критерії

2.2.1 Об'єкт перевірки завдань з аудиту визначається керівництвом та особами, відповідальними за корпоративне управління. Як правило, об'єкт перевірки завдань з аудиту ІС визначається не так точно, як у випадку завдань з фінансового аудиту. Наприклад, об'єкт перевірки завдань з аудиту та підтвердження довіри до ІС може бути як однією системою з інтерфейсами, так і процесом (що охоплює різні системи та інтерфейси), або навіть усією діяльністю певного відділу, пов'язаною з ІС.

2.2.2 Для висловлення своєї професійної думки чи висновків щодо об'єкта перевірки фахівці повинні оцінювати об'єкт перевірки завдань з аудиту за попередньо визначеними критеріями. Фахівці повинні оцінювати такі критерії для забезпечення того, що вони обґрунтовують відповідні твердження.

2.2.3 Один критерій може бути пов'язаним із багатьма твердженнями, і навпаки, одне твердження може вимагати наявності багатьох критеріїв, які разом є частиною забезпечення впевненості в досягненні тверджень.

2.2.4 Якщо фахівці роблять висновок, що критерії забезпечують виконання усіх відповідних тверджень не повністю, вони повинні запропонувати зміну існуючих критеріїв або додаткові критерії. Керівництво аудиту та підтвердження довіри до ІС переглядає та затверджує або відхиляє нові або змінені критерії.

2.2.5 Після оцінювання того, чи критерії повністю забезпечують виконання відповідних тверджень, фахівці повинні також оцінити, чи можна здійснити об'єктивний аналіз і вимірювання таких критеріїв згідно зі Стандартом 1008 «Критерії».

2.3 Твердження, зроблені третіми особами

2.3.1 Організації, які залучають до діяльності третіх осіб на підрядній основі, отримуватимуть звіти про контрольне середовище такої діяльності. Керівництво повинно розглядати кожен з таких звітів для визначення того, чи:
- звіт видано відповідним незалежним професійним органом;
- аудиторська думка є кваліфікованою;
- обсяг цілей контролів адекватно відображає контролі, які вимагає організація;
- часові рамки проведення аудиту відповідають очікуванням організації;
- певні проблеми порушення контролів (які не призвели до загального оцінювання звіту) є придатними для організації;
- твердження, що застосовуються, відповідають необхідним твердженням.

Керівництво аудиту та підтвердження довіри до ІС повинно документально оформляти здійснений аналіз та зроблені висновки. Фахівці повинні забезпечувати перевірку та офіційне схвалення керівництвом тверджень в рамках виконання таких завдань з аудиту, в обсязі яких є

2007 Твердження (продовження)

2.3 Твердження, зроблені третіми особами (продовження)

діяльність, до якої залучаються треті особи. Подальші вказівки щодо цього питання наведено у Стандарті 1206 «Залучення інших експертів».

2.4 Висновки та звіти

2.4.1 Після оцінювання об'єкта перевірки завдань з аудиту за відповідними критеріями фахівці повинні зробити висновки про кожне твердження, ґрунтуючись на сукупних результатах щодо відповідних критеріїв та на власних професійних судженнях.

2.4.2 Після формулювання висновків фахівці повинні видати непрямий чи прямий звіт щодо об'єкта перевірки:

- **непрямий звіт** (щодо тверджень про об'єкт перевірки; наприклад, щодо «повноти» тверджень складової об'єкта перевірки: «На основі здійсненої нами перевірки ефективності діяльності ми вважаємо, що всі значні аспекти змін системи ІТ, які вводяться в дію, повністю зафіксовані у програмі стеження за управлінням змінами у відповідності до обраних критеріїв.»);
- **прямий звіт** (безпосередньо щодо об'єкта перевірки; наприклад, щодо всього об'єкта перевірки: «На основі здійсненої нами перевірки ми вважаємо, що всі значні аспекти змін системи ІТ відповідають процедурі управління змінами у відповідності до обраних критеріїв.»).

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами
3.2 Зв'язок із процесами COBIT 5
3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA, які безпосередньо обґрунтовуються цією настановою;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1007 Твердження	Фахівці з аудиту та підтвердження довіри до ІС повинні перевіряти твердження, на основі яких здійснюватиметься оцінювання об'єкта перевірки, для визначення того, чи такі твердження можна піддати аудиту, і чи є вони достатніми, обґрунтованими та відповідними.
1008 Критерії	Фахівці з аудиту та підтвердження довіри до ІС повинні визначити такі критерії, за якими оцінюватиметься об'єкт перевірки, що будуть об'єктивними, повними, відповідними, зрозумілими, загальновизнаними, достовірними, вимірюваними та будуть дохідливими і доступними для всіх читачів чи користувачів звіту.
1204 Суттєвість	У своїх звітах фахівці з аудиту та підтвердження довіри до ІС повинні розкривати наступне: • відсутність контролів чи їх неефективність; • значущість проблеми порушення контролів; • ймовірність того, що такі вразливі місця призведуть до значного порушення чи суттєвого недоліку.
1206 Залучення інших експертів	У рамках виконання своїх завдань фахівці з аудиту та підтвердження довіри до ІС повинні визначати, переглядати та оцінювати роботу інших експертів, а також документально оформляти висновки щодо обсягу залучення таких експертів та покладання на результати їх роботи.

2007 Твердження (продовження)

3.1 Зв'язок зі стандартами (продовження)

Назва стандарту	Відповідні положення стандарту
1401 Звітування	Фахівці з аудиту та підтвердження довіри до ІС повинні звітувати про результати виконаних завдань, включаючи: • ідентифікацію організації, припустимого одержувача та будь-які обмеження щодо змісту та розповсюдження; • обсяг, цілі та період виконання завдань, а також характер, визначення терміну проведення та обсягу роботи, що підлягає здійсненню; • результати, висновки та рекомендації; • будь-які кваліфікації фахівців з аудиту та підтвердження довіри до ІС чи обмеження обсягу робіт, що стосуються виконання завдань; • підпис, дату та розповсюдження згідно з умовами статуту аудиту чи контракту.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
• Процеси COBIT 5
• Цілі процесів COBIT 5
Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
EDM01 Забезпечувати впровадження та підтримку основних положень корпоративного управління	Забезпечити єдиний підхід, інтегрований та узгоджений з підходом організації до корпоративного управління. Приймати такі рішення у сфері IT, які відповідатимуть стратегіям і цілям організації. Здійснювати ефективний та прозорий нагляд за процесами, пов'язаними з IT, та підтверджувати їх відповідність законодавчим і регуляторним вимогам, а також забезпечити дотримання членами керівної ради вимог до корпоративного управління.
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
• у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
• у керівництва;
• в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
• в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

2007 Твердження (продовження)

4. Термінологія

Термін	Визначення
Критерії	Стандарти та показники, що застосовуються для вимірювання та представлення об'єкта перевірки, відповідно до яких аудитор ІС оцінює об'єкт перевірки. Критерії повинні бути: • об'єктивними (неупередженими); • повними (такими, що містять усі відповідні фактори для того, щоб зробити висновок); • відповідними (такими, що відносяться до об'єкта перевірки); • вимірними (такими, що передбачають постійне вимірювання); • зрозумілими. В атестаційних завданнях можуть оцінюватися показники, які були визначені керівництвом як письмові твердження щодо об'єкта перевірки. Практикуючий фахівець готує свій висновок щодо об'єкта перевірки виходячи з відповідних критеріїв.
Об'єкт перевірки	Певний інформаційний об'єкт, що розглядається в аудиторському звіті та при здійсненні відповідних процедур, стосовно, наприклад, розробки або діяльності внутрішніх контролів та відповідності порядку або стандартам захисту комерційних таємниць та відповідним законам і нормативним документам (сфера діяльності).
Професійні судження	Застосування відповідних знань і досвіду при інформованому прийнятті рішень про напрямки дій, що відповідають обставинам завдань з аудиту та підтвердження довіри до ІС.
Твердження	Будь-яке офіційне висловлювання чи ряд висловлювань керівництва про об'єкт перевірки. Як правило, твердження наводяться у письмовій формі і містять список певних характеристик конкретного об'єкта перевірки або процесу, у який його залучено.

5. Дата набуття чинності

5.1 Дата набуття чинності

Цей переглянутий принцип є чинним для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2008 Критерії

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови полягає у сприянні фахівцям з аудиту та підтвердження довіри до ІС при виборі критеріїв, за якими оцінюватиметься об'єкт перевірки, які є придатними, доступними і з відповідного джерела.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1007 Твердження
1.2.2 Стандарт 1008 Критерії

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані із завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Вибір і застосування критеріїв
2.2 Придатність
2.3 Прийнятність
2.4 Джерело
2.5 Зміна критеріїв під час виконання завдань з аудиту

2.1 Вибір і застосування критеріїв

2.1.1 Фахівці повинні обирати критерії, за якими оцінюватиметься об'єкт перевірки. При виборі критеріїв фахівці повинні з особливою ретельністю розглядати їх придатність, прийнятність і джерела згідно з параграфами 2.2, 2.3 і 2.4, відповідно.

2.1.2 Фахівці повинні ретельно підходити до вибору критеріїв. Оскільки важливо дотримуватися місцевих законів і нормативних документів, і це повинно бути обов'язковою вимогою. Вважається, що багато завдань з аудиту охоплюють такі сфери, як управління змінами, загальні контролі ІТ і контролі доступу, які не керуються законами та нормативними документами. Окрім того, деякі галузі, як, наприклад, галузь платіжних карток, встановили обов'язкові вимоги. Необхідно враховувати відповідність місцевих правил щодо захисту даних і нормативних документів про конфіденційність інформації відповідним міжнародним. Якщо законодавчі вимоги є основоположним принципом, фахівці повинні забезпечити відповідність обраних критеріїв цілям завдань.

2.1.3 Для забезпечення належного оцінювання об'єкта перевірки необхідно застосовувати придатні та прийнятні критерії. Без застосування правильних критеріїв будь-яка професійна думка або висновок можуть призвести до неправильного розуміння або тлумачення їх читачами.

2.1.4 Фахівці повинні утримуватися від оцінювання об'єкта перевірки, ґрунтуючись на власних очікуваннях, досвіді або судженнях, оскільки тоді критерії не будуть вважатися придатними та прийнятними.

2.1.5 Якщо критерії є важкодоступними, неповними або потребують пояснень, фахівці повинні надавати опис або будь-яку іншу інформацію, необхідну для того, щоб звіт був справедливим, об'єктивним і зрозумілим, а також описував контекст, у якому застосовуються критерії.

2.1.6 Фахівці повинні застосовувати свої професійні судження для підтвердження того, що у випадку

2008 Критерії (продовження)

2.1 Вибір і застосування критеріїв (продовження)

використання критеріїв за допомогою них буде надано справедливу та об'єктивну професійну думку або висновки, які не будуть дезінформувати читачів і користувачів. Допускається, що керівництво може задавати такі критерії, які не відповідають усім вимогам.

2.2 Придатність

2.2.1 Фахівці повинні визначати придатність і прийнятність критеріїв, що застосовуються при оцінюванні об'єкта перевірки. Наприклад, нижченаведений критерій застосовується для пояснення наступних критеріїв якісних характеристик: «Згідно з місцевими законами при проведенні операцій з даними будь-яка особиста інформація клієнтів повинна завжди залишатись конфіденційною.»:

- **об'єктивність** (критерії повинні бути неупередженими, щоб не впливати на результати та висновки фахівців і, відповідно, не дезінформувати користувачів аудиторського звіту; наприклад, критерій є об'єктивним, оскільки він затверджений місцевим законом);
- **повнота** (критерії повинні бути повними, щоб при проведенні завдань з аудиту визначати і застосовувати усі критерії, які можуть впливати на висновки фахівців про об'єкт перевірки; таким чином, необхідно, щоб усі критерії, що застосовуються, були повними, враховуючи цілі завдань з аудиту);
- **відповідність** (критерії повинні бути відповідними об'єкту перевірки і сприяти отриманню результатів і висновків, що відповідають цілям завдань з аудиту; критерії можуть залежати від контексту; навіть у випадку однакового об'єкта перевірки критерії можуть різнитися залежно від цілей та обставин завдань з аудиту; наприклад, критерій вважається відповідним , оскільки операції з даними проводяться в рамках обсягу такого завдання з аудиту);
- **можливість здійснювати вимірювання** (у випадку застосування критеріїв різними фахівцями за таких самих умов вони повинні однаково вимірювати об'єкт перевірки і робити однакові висновки; наприклад, критерій є таким, що дозволяє здійснити вимірювання, тому що будь-яку операцію з даними, пов'язаними з незахищеною персональною інформацією, можна виявити єдиним способом і виміряти відповідним чином);
- **зрозумілість** (критерії повинні бути чіткими і не мати значущих відмінностей при їх тлумаченні цільовими користувачами; наприклад, критерій є зрозумілим, оскільки цей розділ закону вже неодноразово розглядався у судовій практиці, і було встановлене чітке розуміння практичного застосування та тлумачення такого закону).

2.3 Прийнятність

2.3.1 На прийнятність критеріїв впливає їх доступність для користувачів аудиторських звітів. Таким чином, користувачі повинні розуміти основи діяльності з підтвердження довіри та відповідність результатів і висновків фахівців. Джерела можуть містити критерії, які є:

- **загальновизнаними** (щоб цільові користувачі не ставили під сумнів їхнє застосування);
- **достовірними** (щоб відображати офіційні положення у відповідній сфері та відповідати об'єкту перевірки; наприклад, офіційні положення можуть публікуватися професійними організаціями, галузевими групами, урядовими або регуляторними органами);
- **загальнодоступними** (включати стандарти, розроблені професійними бухгалтерськими та аудиторськими органами, такими як ISACA, IFAC та іншими загальновизнаними урядовими або професійними органами);
- **доступними для всіх користувачів** (якщо критерії не є загальнодоступними, їх необхідно описати для всіх користувачів у підрозділі «Твердження», який є частиною звіту; твердження складаються з положень про об'єкт перевірки, які відповідають вимогам «критеріїв придатності» і можуть перевірятися згідно зі Стандартом 1007 «Твердження»).

2.3.2 Фахівці повинні забезпечити те, що критерії, які застосовуються при виконанні завдань з аудиту:

- **приймаються ззовні** (є загальновизнаними, достовірними та загальнодоступними);
- **підтверджуються ззовні** (критерії, розроблені керівництвом для окремого завдання з аудиту, не вважаються загальновизнаними, достовірними та загальнодоступними; до їх застосування такі критерії повинні затверджуватися ззовні незалежною визнаною третьою особою з метою підтвердження того, що керівництво потенційно не сприяє отриманню бажаних результатів завдань з аудиту).

2008 Критерії (продовження)

2.4 Джерела

2.4.1 При виборі критеріїв підтвердження довіри до ІС, окрім придатності та доступності, необхідно також розглядати джерела, враховуючи їх застосування та потенційну аудиторію. Наприклад, у випадку державного регулювання найбільш прийнятно обрати критерії, що базуються на твердженнях щодо об'єкта перевірки, розроблених законодавчими чи регуляторними органами. В інших випадках придатними будуть критерії галузевих чи торгових асоціацій. Нижче наведено можливі джерела критеріїв у порядку їх розгляду.

- **Критерії, встановлені ISACA,** – це загальнодоступні критерії та стандарти, які пройшли рецензування і ретельний процес комплексної перевірки загальновизнаними міжнародними експертами у сфері корпоративного управління, контролю, безпеки та підтвердження довіри до ІТ.
- **Критерії, встановлені іншими експертними органами,** схожі на стандарти та критерії ISACA. Вони відповідають об'єкту перевірки і були розроблені та пройшли рецензування і ретельний процес комплексної перевірки експертами у різних сферах.
- **Критерії, встановлені законодавчими чи регуляторними органами,** необхідно застосовувати з обережністю, оскільки закони та нормативні документи можуть бути основою критеріїв. Часто їх формулювання є комплексними і несуть специфічне юридичне значення. У багатьох випадках вимоги необхідно формулювати як твердження. У подальшому свою професійну думку щодо законів, як правило, виражають виключно фахівці у сфері юриспруденції.
- **Критерії, встановлені організаціями без дотримання процесуальних норм,** включають в себе відповідні критерії, розроблені іншими організаціями без дотримання процесуальних норм, загальних обговорень і дискусій.
- **Критерії, розроблені виключно для виконання завдань з аудиту,** необхідно застосовувати з особливою обережністю, щоб вони відповідали критеріям придатності, зокрема, повноти, можливості здійснення вимірювань та об'єктивності. Такі критерії подаються у формі тверджень. Як правило, вони розробляються відповідно до потреб конкретних користувачів. Наприклад, при встановленні критеріїв оцінювання ефективності системи внутрішніх контролів можуть застосовуватися різні основні положення; проте, певні користувачі можуть розробити низку критеріїв, що відповідатимуть їх особливим потребам, наприклад, ієрархії затвердження повноважними особами. В аудиторському звіті фахівці повинні чітко зазначати, що певні критерії розроблено виключно для виконання завдань з аудиту. Вони повинні враховувати, чи такі критерії можуть дезінформувати цільових користувачів і, за необхідності, надати детальнішу інформацію про них. Якщо такі критерії розроблені керівництвом, згідно з параграфом 2.3.2 у звіті необхідно вказувати і звертатися до їх підтвердження ззовні.

2.5 Зміна критеріїв під час виконання завдань з аудиту

2.5.1 При проведенні аудиту додаткова інформація та вивчення об'єкта перевірки можуть призвести до зміни обраних критеріїв:

- певні критерії можуть стати непотрібними для досягнення цілей аудиту; за таких обставин відпадає потреба у подальшій аудиторській роботі, пов'язаній з такими критеріями;
- може виникнути потреба у додаткових критеріях для досягнення цілей аудиту; за таких обставин обираються додаткові критерії, і проводиться аудиторська робота, пов'язана з такими критеріями.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами
3.2 Зв'язок із процесами COBIT 5
3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA, які безпосередньо обґрунтовуються цією настановою;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

2008 Критерії (продовження)

3.1 Зв'язок зі стандартами (продовження)

Назва стандарту	Відповідні положення стандарту
1007 Твердження	Фахівці з аудиту та підтвердження довіри до ІС повинні перевіряти твердження, на основі яких здійснюватиметься оцінювання об'єкта перевірки, для визначення того, чи такі твердження можна перевірити, і чи є вони достатніми, обґрунтованими та відповідними.
1008 Критерії	Фахівці з аудиту та підтвердження довіри до ІС повинні визначити такі критерії, за якими оцінюватиметься об'єкт перевірки, що будуть об'єктивними, повними, відповідними, вимірними, зрозумілими, загальновизнаними, достовірними і доступними для всіх читачів чи користувачів звіту.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
- Процеси COBIT 5
- Мета процесів COBIT 5

Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
EDM01 Забезпечувати впровадження та підтримку основних положень корпоративного управління	Забезпечити єдиний підхід, інтегрований та узгоджений з підходом організації до корпоративного управління. Приймати такі рішення у сфері IT, які відповідатимуть стратегіям і цілям організації. Здійснювати ефективний та прозорий нагляд за процесами, пов'язаними з IT, та підтверджувати їх відповідність законодавчим і регуляторним вимогам, а також забезпечити дотримання членами керівної ради вимог до корпоративного управління.
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
- у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

2008 Критерії (продовження)

4. Термінологія

Термін	Визначення
Критерії	Стандарти та показники, що застосовуються для вимірювання та представлення об'єкта перевірки, відповідно до яких аудитор ІС оцінює об'єкт перевірки. Критерії повинні бути: • об'єктивними (неупередженими); • повними (такими, що містять усі відповідні фактори для того, щоб зробити висновок); • відповідними (такими, що відносяться до об'єкта перевірки); • вимірними (такими, що передбачають постійне вимірювання); • зрозумілими. В атестаційних завданнях можуть оцінюватися показники, які були визначені керівництвом як письмові твердження щодо об'єкта перевірки. Практикуючий фахівець готує свій висновок щодо об'єкта перевірки виходячи з відповідних критеріїв.
Об'єкт перевірки	Певний інформаційний об'єкт, що розглядається в аудиторському звіті та при здійсненні відповідних процедур, стосовно, наприклад, розробки або діяльності внутрішніх контролів та відповідності порядку або стандартам захисту комерційних таємниць та відповідним законам і нормативним документам (сфера діяльності).
Професійні судження	Застосування відповідних знань і досвіду при інформованому прийнятті рішень про напрямки дій, що відповідають обставинам завдань з аудиту та підтвердження довіри до ІС.
Твердження	Будь-яке офіційне висловлювання чи ряд висловлювань керівництва про об'єкт перевірки. Як правило, твердження наводяться у письмовій формі і містять список певних характеристик конкретного об'єкта перевірки або процесу, у який його залучено.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

Настанови з ефективності

Настанови з ефективності:

2201 Планування завдань
2202 Оцінювання ризиків при плануванні аудиту
2203 Ефективність і нагляд
2204 Суттєвість
2205 Докази
2206 Залучення інших експертів
2207 Невідповідності та незаконні дії
2208 Вибірка

Усі настанови описані тут вичерпно. Посилання на окремі стандарти можна отримати на наступній сторінці: www.isaca.org/standard.

2201 Планування завдань

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Ця настанова надає вказівки фахівцям з аудиту та підтвердження довіри до ІС. Адекватне планування сприяє забезпеченню належної уваги до важливих сфер аудиту, виявлення і своєчасного вирішення потенційних проблем, а також до правильної організації, управління та ефективного і продуктивного виконання завдань з аудиту.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1201 Планування завдань
1.2.2 Стандарт 1202 Оцінювання ризиків при плануванні аудиту
1.2.3 Стандарт 1203 Ефективність і нагляд
1.2.4 Стандарт 1204 Суттєвість

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані зі завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 План аудиту ІС
2.2 Цілі
2.3 Обсяг і знання справи
2.4 Ризик-орієнтований підхід
2.5 Документальне оформлення проектного плану завдань з аудиту
2.6 Зміни протягом здійснення аудиту

2.1 План аудиту ІС

2.1.1 Згідно із функцією аудиту необхідно щонайменше щорічно розробляти та оновлювати детальний ризик-орієнтований план аудиту ІС. Річний план повинен встановлювати та описувати багаторічні часові інтервали (від трьох до п'яти років). Багаторічні та річні плани повинні бути основою діяльності з аудиту та підтвердження довіри до ІС та розглядати обов'язки, встановлені у статуті аудиту.

2.1.2 План аудиту ІС необхідно готувати таким чином, щоб він відповідав усім відповідним зовнішнім вимогам і діючим стандартам ISACA.

2.1.3 Кожне завдання з аудиту повинно посилатися на план аудиту ІС або певні розпорядження, цілі та інші відповідні аспекти роботи, що підлягає виконанню.

2.2 Цілі

2.2.1 Для ефективного виконання завдань з аудиту фахівці повинні визначати їх цілі та документально оформляти останні у проектному плані завдань з аудиту. Цілі завдань необхідно встановлювати, враховуючи ризики, пов'язані з діяльністю, що перевіряється.

2.2.2 Фахівці повинні розробляти проектний план завдань з аудиту, який враховує цілі завдань з аудиту. Такі цілі можуть впливати на завдання з аудиту, наприклад, на необхідні ресурси, часові рамки та заплановані результати.

2201 Планування завдань (продовження)

2.3 Обсяг і знання справи

2.3.1 До початку виконання завдань з аудиту необхідно спланувати роботу фахівців таким чином, щоб вона відповідала цілям аудиту. В рамках процесу планування фахівці повинні отримати розуміння організації та її процесів. Це сприятиме визначенню ними значущості ресурсів, що перевіряються, стосовно цілей організації. Таким чином, фахівці можуть зосередити увагу на сферах, які є найбільш чутливими до шахрайських або помилкових практик. Вони повинні визначати обсяг аудиторської роботи, а також здійснювати попереднє оцінювання внутрішніх контролів функції, що перевіряється.

2.3.2 Фахівці повинні отримати розуміння типів персоналу, подій, операцій та практик, що можуть значним чином впливати на певну організацію, функцію, процес або дані, які є об'єктом завдань з аудиту. Знання організації означає розуміння комерційних і фінансових ризиків, які постають перед організацією, а також умов ринкової ніші організації та обсягу покладання організації на залучення підрядників для досягнення своїх цілей. Фахівці повинні застосовувати цю інформацію при визначенні потенційних проблем, формулюванні цілей та обсягу роботи, виконанні роботи та розгляді дій керівництва, до яких вони повинні бути особливо уважними.

2.4 Ризик-орієнтований підхід

2.4.1 Фахівці повинні розробляти проектний план завдань з аудиту для зменшення ризиків аудиту до прийнятного рівня.

2.4.2 Необхідно здійснювати оцінювання ризиків для забезпечення достатньої впевненості у тому, що протягом виконання завдань з аудиту будуть належним чином враховані всі значні питання, а фахівці зможуть зробити висновки. Таке оцінювання повинне визначати сфери з відносно високою ймовірністю існування значних проблем.

2.4.3 За необхідності, потрібно здійснювати оцінювання ризиків і встановлювати пріоритети ризиків, виявлених у сфері, що перевіряється, та середовищі ІС організації.

2.4.4 Як правило, у процесі планування фахівці повинні визначити рівні планування суттєвості таким чином, щоб аудиторська робота була достатньою для досягнення цілей аудиту та ефективно використовувала ресурси аудиту. Наприклад, перевіряючи існуючу систему, фахівці повинні оцінювати суттєвість різних компонентів такої системи при плануванні завдань з аудиту для роботи, що підлягає виконанню. При визначенні суттєвості необхідно враховувати як якісний, так і кількісний аспекти.

2.4.5 До початку виконання завдань з аудиту та протягом здійснення аудиту фахівці повинні враховувати відповідність діючим законам і професійним стандартам аудиту.

2.4.6 Якщо фахівці оцінюють внутрішні контролі з метою покладання на процедури перевірки контролю при підтвердженні інформації, що збирається в рамках більшої аудиторської задачі (наприклад, аудиту історичної фінансової інформації), як правило, вони повинні здійснити попереднє оцінювання контролів і розробити проектний план завдань з аудиту, ґрунтуючись на такому оцінюванні.

2.5 Документальне оформлення проектного плану завдань з аудиту

2.5.1 Робоча документація фахівців повинна містити проектний план завдань з аудиту.

2.5.2 Чітке визначення проекту є ключовим фактором успіху, що забезпечує ефективність і дієвість проекту. В рамках поставлених задач проектний план завдань з аудиту повинен описувати наступне:

- сфери, що підлягають аудиту;
- тип запланованої роботи;
- високорівневі цілі та обсяг роботи;
- опитування, що будуть виконуватись для встановлення фактів;
- належну інформацію, що буде отримана;
- процедури перевірки і затвердження отриманої інформації та їх застосування в ролі аудиторських доказів;
- загальні теми, наприклад:
  - бюджет;
  - наявність і розподіл ресурсів;
  - планові періоди;
  - типи звітів;
  - цільову аудиторію;
  - очікувані результати;
- конкретні теми, наприклад:
  - визначення інструментів, необхідних для збору доказів, проведення тестувань і підготовку / підсумовування інформації для формування звітності;

2201 Планування завдань (продовження)

2.5 Документальне оформлення проектного плану завдань з аудиту (продовження)

– критерії оцінювання, які будуть застосовуватися;
– вимоги до звітування та розповсюдження;
• за необхідності, інші загальні аспекти роботи.

2.5.3 Для виконання завдань з аудиту в рамках встановленого графіку проектний план повинен описувати вимоги до часових рамок завдань з аудиту, як, наприклад, звітний період і різні дати завершення робіт, а також бюджетні витрати.

2.5.4 Фахівці повинні забезпечити повне покриття необхідних компетенцій ресурсами завдання з аудиту. Вони повинні створити групу для виконання завдань з аудиту, яка володітиме необхідними знаннями, навичками та досвідом для успішного виконання завдань з аудиту. Фахівці повинні призначати різні ролі та обов'язки тим членам групи, що займається аудитом ІС, компетенції яких є найбільш відповідними. Детальнішу інформацію можна знайти у Стандарті 1203 «Ефективність і нагляд».

2.5.5 Проектний план завдань з аудиту повинен містити перелік усіх очікуваних результатів, пов'язаних із завданнями з аудиту.

2.5.6 Проектний план завдань з аудиту та усі його подальші зміни повинні затверджуватися керівництвом аудиту та підтвердження довіри до ІС.

2.5.7 Після затвердження керівництвом аудиту та підтвердження довіри до ІС необхідно своєчасно звітувати організації, що підлягає аудиту, про частини проектного плану завдань з аудиту (наприклад, обсяг, часові рамки, документально оформлені вимоги, графік опитувань тощо), щоб вона забезпечила належний та повний доступ і наявність усіх необхідних документів і ресурсів.

2.6 Зміни протягом здійснення аудиту

2.6.1 За необхідності, проектний план завдань з аудиту повинен оновлюватися та змінюватися протягом виконання таких завдань.

2.6.2 Планування завдань з аудиту є безперервним повторюваним процесом. Внаслідок настання непередбачуваних подій, змін умов або отримання аудиторських доказів фахівці можуть зіткнутися з потребою змінити запланований характер, часові рамки та обсяг подальших аудиторських процедур.

2.6.3 План аудиту повинен розглядати можливість настання непередбачуваних подій, які можуть становити ризик для організації. Відповідно, необхідно, щоб проектний план завдань з аудиту міг встановлювати пріоритети таких подій в рамках процесів аудиту та підтвердження довіри, які ґрунтуються на оцінці ризиків.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:
3.1 Зв'язок зі стандартами
3.2 Зв'язок із процесами COBIT 5
3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:
• найбільш придатні стандарти ISACA, які безпосередньо стосуються цієї настанови;
• положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

2201 Планування завдань (продовження)

3.1 Зв'язок зі стандартами (продовження)

Назва стандарту	Відповідні положення стандарту
1201 Планування завдань	Фахівці з аудиту та підтвердження довіри до ІС повинні планувати кожне завдання з аудиту та підтвердження довіри до ІС таким чином, щоб воно відповідало: • цілі (цілям), обсягу, часовим рамкам та очікуваним результатам; • діючим законам і професійним стандартам аудиту; • застосуванню ризик-орієнтованого підходу, де це можливо; • питанням, що виникають у зв'язку зі специфікою завдань; • вимогам до документації та звітності. Фахівці з аудиту та підтвердження довіри до ІС повинні розробляти та документально оформляти проектний план завдань з аудиту та підтвердження довіри до ІС, що описує: • характер, цілі та часові рамки завдань, а також потреби у ресурсах; • терміни проведення та обсяг аудиторських процедур, необхідних для виконання завдань.
1202 Оцінювання ризиків при плануванні аудиту	Функція аудиту та підтвердження довіри до ІС повинна застосовувати необхідний підхід до оцінювання ризиків та відповідну допоміжну методику, щоб розробити загальний план аудиту ІС і визначити пріоритети для ефективного розподілу ресурсів аудиту ІС. При плануванні індивідуальних завдань фахівці з аудиту та підтвердження довіри до ІС повинні визначати та оцінювати ризики, пов'язані зі сферою, що перевіряється.
1203 Ефективність і нагляд	Фахівці з аудиту та підтвердження довіри до ІС повинні здійснювати роботу за узгодженим графіком у відповідності до затвердженого плану аудиту ІС, щоб охопити виявлені ризики.
1204 Суттєвість	При плануванні завдань фахівці з аудиту та підтвердження довіри до ІС повинні враховувати потенційні вразливі місця та відсутність контролів, а також те, чи такі вразливі місця та відсутність контролів можуть призвести до значного порушення чи суттєвого недоліку.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
• Процеси COBIT 5
• Мета процесів COBIT 5
Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
MEA01 Відстежувати, оцінювати та аналізувати ефективність та відповідність	Забезпечити прозорість виконання та відповідності, а також сприяти досягненню цілей.
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.
MEA03 Відстежувати, оцінювати та аналізувати відповідність зовнішнім вимогам	Забезпечити дотримання організацією діючих зовнішніх вимог.

2201 Планування завдань (продовження)

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:

- у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Оцінювання ризиків	Процес визначення та оцінювання ризиків та їх потенційного впливу. Оцінювання ризиків здійснюється для визначення складових або сфер, які представляють найбільший ризик, уразливість або вплив на організацію, для включення до щорічного плану аудиту ІС. Оцінювання ризиків також використовується для управління ризиками, пов'язаними зі здійсненням проекту та його вигодами.
План аудиту	1.План, що описує характер, часові рамки та обсяг аудиторських процедур, які виконуватимуться членами групи, що виконує завдання, для отримання достовірних і достатніх аудиторських доказів для формування висновку. **Обмежуюча примітка.** Він описує сфери, що підлягають аудиту, тип запланованої роботи, високорівневі цілі та обсяг роботи, а також такі теми, як бюджет, розподіл ресурсів, планові періоди, типи звітів, цільову аудиторію та інші загальні аспекти роботи. 2.Високорівневий опис аудиторської роботи, що підлягає виконанню в рамках певного періоду часу.
Ризик аудиту	Ризик дійти до хибного висновку ґрунтуючись на результатах аудиту. Є три складових ризику аудиту: • ризик системи контролю; • ризик не виявлення ; • ризик, притаманний організації.
Суттєвість	Аудиторська концепція важливості елемента інформації, враховуючи її вплив чи наслідки на функціонування об'єкта перевірки в цілому. Вираження відносної значущості чи важливості окремого питання в контексті організації в цілому.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2202 Оцінювання ризиків та планування аудиту

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Рівень аудиторської роботи, необхідний для досягнення цілей аудиту, є суб'єктивним рішенням, яке приймають фахівці з аудиту та підтвердження довіри до ІС. Мета цієї настанови полягає у зменшенні ризику неправильних висновків на основі результатів аудиту та існування помилок у сфері, що підлягає аудиту.

1.1.2 Ця настанова надає вказівки щодо застосування підходу оцінювання ризиків з метою розробки:
- плану аудиту ІС, що охоплює усі річні завдання з аудиту;
- проектного плану завдань з аудиту, зосередженому на одному окремому завданні з аудиту.

1.1.3 Ця настанова описує різні типи ризиків, які постають перед фахівцями з аудиту та підтвердження довіри до ІС.

1.1.4 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1201 Планування завдань
1.2.2 Стандарт 1202 Оцінювання ризиків при плануванні
1.2.3 Стандарт 1203 Ефективність і нагляд
1.2.4 Стандарт 1204 Суттєвість
1.2.5 Стандарт 1207 Невідповідності та незаконні дії

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані зі завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Оцінювання ризиків плану аудиту ІС
2.2 Методика оцінювання ризиків
2.3 Оцінювання ризиків окремих завдань з аудиту
2.4 Ризики аудиту
2.5 Ризик, притаманний організації
2.6 Ризик системи контролю
2.7 Ризик невиявлення помилок

2.1 Оцінювання ризиків плану аудиту ІС

2.1.1 При розробці загального плану аудиту ІС необхідно слідувати відповідному підходу оцінювання ризиків. Оцінювання ризиків необхідно здійснювати і документально оформляти щорічно з метою сприяння процесу розробки плану аудиту ІС, враховуючи організаційні стратегічні плани та цілі, а також структуру управління ризиками та ініціативи організації.

2.1.2 При розробці плану аудиту ІС фахівці повинні враховувати такі елементи для правильного та повного оцінювання ризиків, пов'язаних із загальним обсягом сфери аудиту ІС:
- повне покриття всіх сфер, що входять в обсяг аудиту ІС, включаючи широкий спектр

2202 Оцінювання ризиків та планування аудиту (продовження)

2.1 Оцінювання ризиків плану аудиту ІС (продовження)

усієї можливої аудиторської діяльності;
- надійність і придатність оцінювання ризиків, передбаченого керівництвом;
- процеси, яким слідує керівництво при контролі, розгляді та звітуванні про можливі ризики чи питання;
- покриття ризиків супутньої діяльності, що стосується діяльності, яка перевіряється.

2.1.3 Застосування підходу до оцінювання ризиків повинно сприяти процесу встановлення пріоритетів і графіків роботи з аудиту та підтвердження довіри до ІС, вибору сфер і складових, які становлять інтерес для аудиту, а також процесу прийняття рішень при розробці та проведенні окремих завдань з аудиту ІС.

2.1.4 Фахівці повинні забезпечити затвердження обраного підходу до оцінювання ризиків особами, відповідальними за корпоративне управління, а також його розповсюдження зацікавленим сторонам.

2.1.5 Фахівці повинні застосовувати оцінювання ризиків для визначення та обґрунтування кількості ресурсів, необхідних для виконання плану аудиту ІС і вимог окремих завдань при проведенні аудиту ІС.

2.1.6 Ґрунтуючись на оцінюванні ризиків, фахівці повинні розробити план аудиту ІС, який буде основою діяльності з аудиту та підтвердження довіри до ІС. Такий план повинен:
- враховувати вимоги та діяльність з аудиту та підтвердження довіри, не пов'язану з ІС;
- оновлюватися щорічно;
- затверджуватися особами, відповідальними за корпоративне управління;
- враховувати обов'язки, встановлені статутом аудиту.

Детальнішу інформацію наведено у Стандарті 1201 «Планування завдань».

2.2 Методика оцінювання ризиків

2.2.1 Для забезпечення повного і точного покриття завдань з аудиту у плані аудиту ІС фахівці повинні розглядати відповідну методику оцінювання ризиків.

2.2.2 Розробляючи методику, фахівці повинні щонайменше здійснювати аналіз ризику, притаманного організації, що відноситься до доступності системи, цілісності даних і конфіденційності комерційної інформації.

2.2.3 Існує багато методик для сприяння процесу оцінювання ризиків від простих класифікацій високого, середнього та низького рівнів ризиків, що ґрунтуються на експертних оцінках фахівців, до більш наукових кількісних підрахунків, що надають кількісні показники ризиків, або ж таких, які поєднують вищезазначені методики. Фахівці повинні розглядати рівень складності та деталі, притаманні організації або об'єкту перевірки. Конкретні вказівки щодо здійснення оцінювання ризиків наведено у виданні ISACA «COBIT 5 про ризики».

2.2.4 Усі методики оцінювання ризиків ґрунтуються певною мірою на суб'єктивних судженнях щодо процесу (наприклад, при визначенні важливості різних параметрів). Фахівці повинні визначати суб'єктивні рішення, необхідні для застосування певних методик, і враховувати, чи можна робити і затверджувати такі судження з достатнім рівнем точності.

2.2.5 При визначенні найбільш відповідної методики оцінювання ризиків фахівці повинні враховувати наступне:
- тип інформації, яку необхідно зібрати (деякі системи застосовують фінансові результати як єдину систему вимірів, що не завжди підходить для завдань з аудиту ІС); • вартість програмного забезпечення або інших ліцензій, необхідних для застосування методики;
- поточний ступінь доступності необхідної інформації;
- кількість додаткової інформації, яку необхідно зібрати для отримання надійних результатів, а також вартість збору такої інформації (включаючи необхідні часові затрати);
- висновки інших користувачів та їхні оцінки щодо корисності методики для покращення ефективності та / або дієвості їхніх аудитів;
- готовність осіб, відповідальних за корпоративне управління у сфері аудиту ІС, прийняти методологію як засіб визначення типу та рівня аудиторської роботи.

2.2.6 Не існує такої методики оцінювання ризиків, яка могла б підійти для всіх ситуацій. Обставини, що впливають на аудит, можуть з часом змінюватися. Фахівці повинні періодично виконувати повторне оцінювання відповідності обраної методики оцінювання ризиків.

2.2.7 Фахівці повинні застосовувати обрані методики оцінювання ризиків при розробці загального плану аудиту ІС та плануванні окремих завдань з аудиту. Оцінювання ризиків необхідно

2202 Оцінювання ризиків та планування аудиту (продовження)

2.2 Методика оцінювання ризиків (продовження)

розглядати у поєднанні з іншими методиками аудиту при прийнятті рішень щодо планування, пов'язаних, наприклад, із наступним:
- сферами або напрямками діяльності, що підлягають аудиту;
- кількістю часу та ресурсів, необхідних для проведення аудиту;
- характером, обсягом і часовими рамками аудиторських процедур.

2.2.8 Затверджена методологія оцінювання ризиків повинна сприяти отриманню прийнятних, обґрунтованих, порівнянних і повторюваних результатів. Оцінювання ризиків, яка здійснюється за допомогою методики, повинна бути прийнятною (за період аудиту), обґрунтованою, порівнянною (з попередніми / наступними оцінками, отриманими за допомогою такої ж методики оцінювання) та повторюваною (за умови такого ж набору фактів така сама методологія оцінювання призведе до отримання аналогічних результатів).

2.3 Оцінювання ризиків окремих завдань з аудиту

2.3.1 При плануванні окремих завдань фахівці повинні визначати та оцінювати ризики, притаманні сфері, що перевіряється. Результати такого оцінювання ризиків повинні відображатися в цілях завдань з аудиту. Оцінюючи ризики, фахівці повинні розглядати:
- результати попередніх завдань з аудиту, перевірок і отриманих даних, у тому числі усіх корегуючи заходів;
- комплексний процес оцінювання ризиків організації;
- ймовірність виникнення окремих ризиків;
- вплив окремих ризиків (у грошових або інших показниках), якщо такі мають місце.

2.3.2 Фахівці повинні забезпечити повне розуміння всього обсягу діяльності до початку оцінювання ризиків. Вони повинні отримати коментарі та пропозиції зацікавлених, а також інших відповідних сторін. Це необхідно для правильного визначення та вивчення впливу можливих ризиків при виконанні завдань з аудиту.

2.3.3 Мета оцінювання ризиків полягає у зменшенні ризиків аудиту до прийнятно низького рівня та у визначенні тих частин діяльності, на які необхідно особливо орієнтуватися під час аудиту. При плануванні та проведенні аудиту ІС це здійснюється за допомогою належного оцінювання об'єкта перевірки ІС і відповідних контролів.

2.3.4 При плануванні окремих процедур аудиту та підтвердження довіри до ІС фахівці повинні враховувати той факт, що чим нижчий поріг суттєвості, тим точніші аудиторські очікування та більші ризики аудиту.

2.3.5 При плануванні окремих процедур аудиту та підтвердження довіри до ІС фахівці повинні враховувати можливі незаконні дії, що можуть вимагати зміни характеру, часових рамок або обсягу існуючих процедур. Детальнішу інформацію наведено у Стандарті 1207 «Невідповідності та незаконні дії» та Настанові 2207.

2.3.6 Для забезпечення додаткової впевненості при високому рівні ризиків аудиту або низькому порогу суттєвості фахівці повинні компенсувати це розширенням обсягу та характеру аудиторських досліджень, пов'язаних з ІС, або розширенням перевірки на суттєвість.

2.4 Аудиторські ризики

2.4.1 Ризики аудиту відносяться до ризику досягнення неправильного висновку, ґрунтуючись на результатах аудиту. Три складових аудиторських ризиків:
- ризик системи контролів;
- ризик невиявлення помилок;
- ризик, притаманний організації.

2.4.2 При визначенні загального рівня ризиків фахівці повинні розглядати їх кожну складову, включаючи ризик, притаманний об'єкту перевірки, у тому числі ризик, притаманний організації, та ризик системи контролю; у поєднанні з ризиком невиявлення помилок вони відносяться до ризиків аудиту. Подальша інформація щодо різних складових ризиків аудиту наведена у параграфах 2.5-2.7.

2.5 Ризик, притаманний організації

2.5.1 Ризик, притаманний організації, – це вразливість сфери аудиту до помилок, які окремо чи у поєднанні з іншими помилками можуть бути суттєвими за умови відсутності відповідних внутрішніх контролів. Наприклад, ризик, притаманний організації, пов'язаний з операційними системами, за умови відсутності відповідних контролів, як правило, є високим, оскільки зміни чи навіть розкриття даних або програм через вразливі місця операційних систем можуть призвести до отримання помилкової інформації керівництва або конкурентних недоліків. Однак, ризик, притаманний організації, пов'язаний з безпекою окремого ПК, що за результатами належного

2202 Оцінювання ризиків та планування аудиту (продовження)

2.5 Ризик, притаманний організації (продовження)

аналізу не використовується для виконання критично важливих для бізнесу призначень, як правило, є низьким.

2.5.2 У більшості сфер аудиту ІС ризик, притаманний організації, є високим, оскільки потенційний вплив помилок, як правило, поширюється на декілька бізнес-систем і на багатьох користувачів.

2.6 Ризик системи контролю

2.6.1 Ризик системи контролю – це ризик виникнення помилок у сфері аудиту, які окремо чи у поєднанні з іншими помилками можуть бути суттєвими, а також яких неможливо уникнути чи своєчасно виявити або виправити за допомогою системи внутрішніх контролів. Наприклад, ризик системи контролю, пов'язаний з ручною перевіркою комп'ютерних протоколів, може бути високим у зв'язку з об'ємом зафіксованої інформації. Ризик системи контролю, пов'язаний із процедурами автоматизованої перевірки даних, як правило, є низьким, оскільки процеси здійснюються послідовно.

2.6.2 Фахівці повинні оцінювати ризик системи контролю як високий, якщо відповідні внутрішні контролі не є:
- виявленими;
- оціненими як ефективні;
- перевіреними та діючими належним чином.

2.6.3 Фахівці повинні враховувати як універсальні, так і детальні контролі ІС.
- Універсальні контролі ІС – це підмножина загальних контролів, що зосереджується на управлінні та відстежуванні середовища ІС. Таким чином, універсальні контролі ІС впливають на всю діяльність, пов'язану з ІС. Їх вплив на роботу фахівців не обмежується забезпеченням надійності контролів прикладних програм у системі бізнес-процесів. Такі контролі також впливають на надійність детальних контролів ІС, наприклад, на розробку прикладних програм, реалізацію системи, управління системою захисту та процедури резервного копіювання. Слабкі універсальні контролі ІС і, відповідно, слабке управління та відстежування середовища ІС повинні звернути увагу фахівців на ймовірність існування високого ризику того, що контролі, розроблені для функціонування на рівні деталей, можуть бути неефективними.
- Детальні контролі ІС складаються з контролів прикладних програм і таких загальних контролів, які не відносяться до універсальних контролів ІС. Згідно з основними положеннями COBIT це – контролі придбання, реалізації, поставки та підтримки систем і послуг, пов'язаних з ІС.

2.6.4 Ризик, який повинні враховувати фахівці, стосується обмежень і недоліків детальних контролів ІС, спричинених невідповідностями універсальних контролів ІС.

2.7 Ризик невиявлення помилок

2.7.1 Ризик невиявлення помилок – це ризик того, що процедури перевірки на суттєвість не виявлять помилок, які окремо чи у поєднанні з іншими помилками можуть бути значними. Наприклад, ризик невиявлення помилок, пов'язаний з визначенням порушень безпеки прикладної системи, як правило, є високим, оскільки протоколи за весь період аудиту недоступні протягом аудиту. Ризик невиявлення помилок, пов'язаний з визначенням відсутності плану відновлення в аварійних ситуаціях, як правило, є низьким, оскільки його наявність легко перевіряється.

2.7.2 При визначенні необхідного рівня перевірки на суттєвість фахівці повинні враховувати:
- оцінювання ризику, притаманного організації;
- висновки щодо ризику системи контролів, отримані після перевірки на відповідність.

2.7.3 Чим вищим оцінюється ризик, притаманний організації, та ризик системи контролю, тим більше аудиторських доказів повинні, як правило, отримати фахівці від виконання процедур перевірки на суттєвість.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами

3.2 Зв'язок із процесами COBIT 5

3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:
- найбільш придатні стандарти ISACA, які безпосередньо стосуються цієї настанови;
- положення стандартів, які є найбільш придатними для цієї настанови.

2202 Оцінювання ризиків та планування аудиту (продовження)

3.1 Зв'язок зі стандартами (продовження)

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1201 Планування завдань	Фахівці з аудиту та підтвердження довіри до ІС повинні планувати кожне завдання з аудиту та підтвердження довіри до ІС таким чином, щоб воно відповідало: • цілі (цілям), обсягу, часовим рамкам і запланованим результатам; • діючим законам і професійним аудиторським стандартам; • застосуванню, за необхідності, ризик-орієнтованого підходу; • питанням, що виникають у зв'язку зі специфікою завдань; • вимогам до документації та звітності.
1202 Оцінювання ризиків при плануванні	Функція аудиту та підтвердження довіри до ІС повинна застосовувати необхідний підхід до оцінювання ризиків та відповідну допоміжну методику, щоб розробити загальний план аудиту ІС і визначити пріоритети для ефективного розподілу ресурсів аудиту ІС. При плануванні індивідуальних завдань фахівці з аудиту та підтвердження довіри до ІС повинні визначати та оцінювати ризики, пов'язані зі сферою, що перевіряється. Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики, пов'язані з об'єктом перевірки, ризики аудиту та інші відповідні ризики для організації.
1203 Ефективність і нагляд	Фахівці з аудиту та підтвердження довіри до ІС повинні здійснювати роботу за узгодженим графіком у відповідності до затвердженого плану аудиту ІС, щоб охопити виявлені ризики.
1204 Суттєвість	При плануванні завдань фахівці з аудиту та підтвердження довіри до ІС повинні враховувати потенційні вразливі місця та відсутність контролів, а також те, чи такі вразливі місця та відсутність контролів можуть призвести до значного порушення чи суттєвого недоліку. При визначенні характеру, часових рамок та обсягу аудиторських процедур фахівці з аудиту та підтвердження довіри до ІС повинні враховувати аудиторську суттєвість та її зв'язок з аудиторськими ризиками. Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати сукупний ефект незначного браку контролів та вразливих місць, а також те, чи така відсутність контролів може перерости у значне порушення чи суттєвий недолік. У своїх звітах фахівці з аудиту та підтвердження довіри до ІС повинні розкривати наступне: • відсутність контролів чи їх неефективність; • значущість проблеми порушення контролів; • ймовірність того, що такі вразливі місця призведуть до значного порушення чи суттєвий недолік.
1207 Невідповідності та незаконні дії	При виконанні завдань фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики існування невідповідностей та незаконних дій.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає такі найбільш придатні , як:
• Процеси COBIT 5
• Цілі процесів COBIT 5
Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

2202 Оцінювання ризиків та планування аудиту (продовження)

3.2 Зв'язок із процесами COBIT 5 (продовження)

Процес COBIT 5	Мета процесу
EDM01 Забезпечувати впровадження та підтримку основних положень корпоративного управління	Забезпечити єдиний підхід, інтегрований та узгоджений з підходом організації до корпоративного управління. Приймати такі рішення у сфері IT, які відповідатимуть стратегіям і цілям організації. Здійснювати ефективний та прозорий нагляд за процесами, пов'язаними з IT, та підтверджувати їх відповідність законодавчим і регуляторним вимогам, а також забезпечити дотримання членами керівної ради вимог до корпоративного управління.
EDM03 Забезпечувати оптимізацію ризиків	Забезпечити, щоб ризики організації, пов'язані з IT, не перевищували рівень її схильності та піддатливості ризикам, вплив ризиків, пов'язаних з IT, на вартість організації визначений і контролюється, а потенціал відхилень, пов'язаних з невідповідностями, мінімізований.
APO12 Управляти ризиками	Поєднати управління ризиками організації, пов'язаними з IT, із загальним управлінням ризиками організації та збалансувати витрати та переваги управління ризиками організації, пов'язаними з IT.
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.
MEA03 Відстежувати, оцінювати та аналізувати відповідність зовнішнім вимогам	Забезпечити дотримання організацією діючих зовнішніх вимог.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:

- у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Детальні контролі ІС	Контролі придбання, реалізації, поставки та підтримки систем і послуг, пов'язаних з ІС, що складаються з контролів прикладних програм і таких загальних контролів, які не відносяться до універсальних контролів ІС.
Оцінювання ризиків	Процес визначення та оцінювання ризиків та їх потенційного впливу. Оцінювання ризиків здійснюється для визначення складових або сфер, які представляють найбільший ризик, уразливість або вплив на організацію, для включення до щорічного плану аудиту ІС. Оцінювання ризиків також використовується для управління ризиками, пов'язаними зі здійсненням проекту та його вигодами.
Перевірка на суттєвість	Отримання аудиторських доказів щодо повноти, точності чи існування діяльності або операцій у період аудиту.
Притаманний ризик	Рівень ризику без урахування заходів, які вжило або може вжити керівництво (наприклад, застосування контролів). Дивіться визначення терміну «ризик системи контролю».

2202 Оцінювання ризиків та планування аудиту (продовження)

Термін	Визначення
Ризик аудиту	Ризик дійти до хибного висновку ґрунтуючись на результатах аудиту. Є три складових ризику аудиту: • ризик системи контролю; • ризик не виявлення помилок; • ризик, притаманний організації.
Ризик невиявлення помилок	Ризик невиявлення процедурами, які використовують фахівці з аудиту та підтвердження довіри до ІС, помилки, яка може бути значною особисто або у поєднанні з іншими помилками. Дивіться визначення терміну «аудиторські ризики».
Ризик системи контролю	Ризик існування значної помилки, яку система внутрішнього контролю не може вчасно виявити або попередити. Дивіться визначення терміну «ризик, притаманний організації».
Статут аудиту	Документ, затверджений особами, відповідальними за корпоративне управління, що визначає мету, повноваження та відповідальність щодо дій внутрішнього аудиту. Статут повинен: • встановлювати роль внутрішнього аудиту в організації; • санкціонувати доступ до документації, персоналу та майна, необхідних для виконання завдань з аудиту ІС та підтвердження довіри до ІС; • визначати сферу діяльності аудиту.
Суттєвість	Аудиторська концепція важливості елемента інформації, враховуючи її вплив чи наслідки на функціонування об'єкта перевірки в цілому. Вираження відносної значущості чи важливості окремого питання в контексті організації в цілому.
Універсальні контролі ІС	Загальні контролі, розроблені для управління та відстежування середовища ІС, та які, відповідно, впливають на всю діяльність, пов'язану з ІС.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2203 Ефективність і нагляд

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Ця настанова надає фахівцям з аудиту та підтвердження довіри до ІС вказівки щодо виконання завдань з аудиту та контролю за членами групи, що займається аудитом ІС. Вона описує:
- виконання завдань з аудиту;
- ролі та обов'язки, а також необхідні знання та навички для виконання завдань з аудиту;
- ключові аспекти нагляду;
- збір доказів;
- документальне оформлення виконаної роботи;
- формулювання результатів і висновків.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1	Стандарт 1005	Належна професійна ретельність
1.2.2	Стандарт 1006	Професійність
1.2.3	Стандарт 1201	Планування завдань
1.2.4	Стандарт 1203	Ефективність і нагляд
1.2.5	Стандарт 1205	Докази
1.2.6	Стандарт 1401	Звітування

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані зі завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Виконання роботи
2.2 Ролі, обов'язки, знання та навички
2.3 Контроль
2.4 Докази
2.5 Документальне оформлення
2.6 Отримані дані та висновки

2.1 Виконання роботи

2.1.1 Фахівці повинні планувати і виконувати кожне завдання з аудиту у відповідності до затвердженого плану аудиту ІС. Створення проектного плану завдань з аудиту, детально описане у Стандарті 1201 «Планування завдань», дозволяє фахівцям зрозуміти всі елементи обсягу, а також необхідні навички та знання для виконання завдань з аудиту в рамках встановленого графіку, враховуючи усі виявлені ризики.

2.1.2 Головні задачі при виконанні завдань з аудиту:
- **планування та оцінювання ризиків** (фахівці повинні виконувати цю діяльність згідно зі Стандартом 1201 «Планування завдань» і Стандартом 1202 «Оцінювання ризиків при плануванні»);
- **визначення контролів** (зважаючи на обсяг, цілі аудиту та головні сфери ризиків, виявлені у плані аудиту ІС, фахівці повинні визначати контролі в обсягу завдань з аудиту);

2203 Ефективність і нагляд (продовження)

2.1 Виконання роботи (продовження)

- **оцінювання контролів і збір доказів** (згідно зі Стандартом 1205 «Докази» фахівці повинні оцінювати контролі обсягу шляхом збору та аналізу інформації та доказів щодо ефективності дизайну та ефективності функціонування контролів);
- **документальне оформлення виконаної роботи і встановлення отриманих даних** (фахівці повинні документально оформляти виконану роботу, фіксувати зібрану інформацію та докази і документально оформляти усі отримані дані);
- **підтвердження отриманих даних і подальший контроль корегуючих заходів** (фахівці повинні підтверджувати отримані ними дані щодо організації, що підлягає аудиту; якщо організація, що підлягає аудиту, застосує корегуючи заходи щодо отриманих даних до завершення завдань з аудиту, фахівці повинні описати такі заходи у своїй документації (та висновках), але, окрім того, в обов'язковому порядку зазначити початкові дані);
- **висновки та звітування** (згідно зі Стандартом 1401 «Звітування» фахівці повинні робити висновки та звітувати про вплив зауважень аудиту на досягнення цілей аудиту; зосередження лише на зауваженнях до системи контролів без оцінювання їх впливу на цілі аудиту є недостатнім).

2.2 Ролі, обов'язки, знання та навички

2.2.1 Під час виконання завдань фахівці, відповідальні за завдання з аудиту, повинні визначати та управляти ролями та обов'язками членів групи, що проводить аудит ІС, розглядаючи, щонайменше:
- розробку методологій і підходів;
- створення програм аудиту;
- виконання та перевірку ролей;
- вирішення питань, ускладнень і проблем у процесі їх виникнення;
- документальне оформлення та роз'яснення отриманих даних;
- написання звітів.

2.2.2 Ґрунтуючись на потребах завдань, відповідальні фахівці повинні враховувати компетенції, необхідні для виконання певних завдань з аудиту. Вони повинні створити групу, що буде виконувати завдання, члени якої колективно володітимуть навичками, знаннями та досвідом для успішного завершення таких завдань. Фахівці повинні призначати різні ролі та обов'язки тим членам групи, що займається аудитом ІС, компетенції яких є найбільш відповідними.

2.2.3 Фахівці повинні приймати лише такі ролі, обов'язки та відповідні задачі, які вони можуть виконати за допомогою своїх знань і навичок. Питання часу і вартості можуть не дозволити фахівцям отримати усі необхідні знання та навички до початку завдань з аудиту; таким чином, фахівці можуть приймати ролі, обов'язки та відповідні задачі, тільки якщо у них є обґрунтовані очікування щодо застосування необхідних заходів для успішного завершення завдань з аудиту. Нижчезазначені заходи допускають існування таких обґрунтованих очікувань:
- навчання під час роботи (за певних обставин фахівці можуть здобути необхідні навички та знання протягом виконання завдань з аудиту);
- контроль (відповідальні фахівці можуть організувати адекватний контроль за членами групи, що проводить аудит ІС, який сприятиме успішному виконанню задач під наглядом);
- зовнішні ресурси (відповідальні фахівці можуть розглянути залучення зовнішніх експертів для виконання завдань з аудиту у тих сферах, в яких у них відсутні адекватні знання та навички; відповідальні фахівці повинні сприяти розвитку внутрішніх членів групи, що проводить аудит ІС, шляхом їх тісної співпраці із зовнішніми експертами з метою передачі їх знань і навичок групі).

2.2.4 Вказівки щодо набуття, підтримки та відстеження необхідних компетенцій детально описані у Стандарті 1006 «Професійність».

2.3 Контроль

2.3.1 Кожна задача, виконана в рамках завдань з аудиту членами групи, що займається аудитом ІС, повинна контролюватися фахівцями, які курують їх, щоб забезпечити її відповідність аудиторським цілям і діючим професійним стандартам аудиту. Необхідний обсяг нагляду залежить від навичок, знань і досвіду фахівців, що виконують задачу під наглядом, а також від складності завдань з аудиту.

2.3.2 Нагляд – це процес, характерний кожному кроку завдань з аудиту, включаючи:
- забезпечення того, що члени групи, що займається аудитом ІС, колективно володіють навичками, знаннями та досвідом для успішного завершення завдань з аудиту;
- забезпечення створення та затвердження відповідного проектного плану завдань з аудиту та програми аудиторської роботи;

2203 Ефективність і нагляд (продовження)

2.3 Контроль (продовження)

- перегляд робочої документації завдань з аудиту;
- забезпечення точного, чіткого, стислого, об'єктивного, конструктивного та своєчасного звітування про завдання з аудиту організації, що підлягає аудиту, та іншим відповідним зацікавленим сторонам;
- забезпечення виконання затвердженої робочої програми завдань з аудиту до завершення таких завдань, якщо зміни до неї не були виправдані та затверджені заздалегідь, а також досягнення цілей завдань з аудиту;
- забезпечення можливості розвитку навичок і знань членів групи, що займається аудитом ІС.

2.3.3 Перегляд робочої документації завдань з аудиту необхідний для забезпечення того, що виконуються всі необхідні аудиторські процедури, збираються достатні та відповідні докази, а висновки належним чином відповідають цілям завдань та висновкам та професійним судженням. Враховуючи цілі такого перегляду, його повинні здійснювати ті члени аудиторської групи, які несуть відповідальність за нагляд роботи фахівців, що створюють робочу документацію завдань з аудиту.

2.3.4 У процесі необхідно фіксувати всі виникаючі питання. При наданні фахівцями рішень чи відповідей на поставлені питання необхідно слідкувати за наявністю достатніх і відповідних доказів для підтвердження того, що такі питання підняли, розглянули та вирішили.

2.3.5 Перегляд відповідних доказів необхідно оформляти документально та зберігати. Крім документального оформлення доказів про здійснення перегляду, з-поміж інших можна виконувати наступні дії:

- датування та завірення підписами усієї робочої документації завдань з аудиту після здійснення перегляду;
- здійснення перевірки робочої документації завдань з аудиту згідно із контрольним списком;
- підготовку підписаного документу, який містить посилання на робочу документацію завдань з аудиту, що перевіряється, та детально описує характер, часові рамки, обсяг і результати перевірки.

Усі ці варіанти є дійсними як в електронному, так і в друкованому вигляді.

2.3.6 Контроль сприяє розвитку та оцінюванню діяльності фахівців. Думка перевіряючих фахівців щодо роботи, яка виконується іншими членами групи, що займається аудитом ІС, є переважаючою і дозволяє детально та адекватно оцінювати діяльність останніх. Перевіряючі фахівці повинні вказувати сфери, які потребують розвитку, а також рекомендувати шляхи вдосконалення навичок і знань.

2.4 Докази

2.4.1 Для формування професійної думки, обґрунтування висновків і, відповідно, досягнення цілей аудиту фахівці повинні отримувати достатні та відповідні докази. Визначення того, чи докази є достатніми та відповідними, повинно ґрунтуватися на важливості цілей аудиту та зусиллях, затрачених на досягнення доказів.

2.4.2 Фахівці повинні отримувати додаткові докази, якщо вони вважають, що отримані докази не відповідають критеріям достатності та відповідності для формування професійної думки, обґрунтування висновків і, відповідно, досягнення цілей аудиту.

2.4.3 Фахівці повинні обирати найбільш відповідні процедури збору доказів залежно від об'єкта аудиту.

2.4.4 Фахівці повинні враховувати джерела та характер отриманих доказів з метою оцінювання їх надійності та необхідності подальшого підтвердження.

2.4.5 Для обґрунтування отриманих даних і формування висновків фахівці повинні виконувати належний аналіз і тлумачення. Отримані докази та інформація повинні розглядатися із врахуванням очікувань, визначених чи зроблених фахівцями. Фахівці повинні враховувати:

- неочікувані відмінності;
- відсутність очікуваних відмінностей;
- шахрайство чи незаконні дії;
- невідповідність законам і нормативним документам;
- незвичну чи неповторювану діяльність.

2.4.6 У випадку виявлення відхилень від очікувань фахівці повинні поцікавитись у керівництва про причини відмінностей. Якщо пояснення керівництва будуть адекватним, фахівці згідно зі своїми професійними судженнями повинні змінити свої очікування і здійснити повторний аналіз доказів та інформації.

2.4.7 Значущі відхилення, які організація, що підлягає аудиту, не може адекватно оцінити, повинні вноситися в результати аудиту та повідомлятися вищому виконавчому керівництву або

2203 Ефективність і нагляд (продовження)

2.4 Докази (продовження)

особам, відповідальним за корпоративне управління. Залежно від обставин фахівці повинні рекомендувати відповідні заходи.

2.4.8 Детальні вказівки щодо різних видів доказів, процедур їх збору, відповідних джерел, шляхів доступу до доказів тощо наведено у Стандарті 1205 «Докази».

2.5 Документальне оформлення

2.5.1 Фахівці повинні своєчасно готувати достатню, відповідну та належну документацію, яка обґрунтовує висновки і містить докази здійсненої перевірки. Достатня, відповідна та належна документація повинна дозволити розсудливій інформованій особі, яка раніше не мала відношення до відповідних завдань з аудиту, знову виконати задачі, що мали місце під час здійснення роботи, та дійти тих самих висновків. Документація повинна містити:

- цілі завдань з аудиту та обсяг роботи;
- проектний план завдань з аудиту;
- програму аудиторської роботи;
- кроки, здійснені під час аудиту;
- зібрані докази;
- висновки і рекомендації.

2.5.2 Документація сприяє плануванню, виконанню та перевірці завдань з аудиту, оскільки вона:

- визначає, хто з членів групи, що займається аудитом ІС, виконав кожну аудиторську задачу, та роль цієї особи у підготовці та перевірці документації;
- фіксує необхідні докази;
- забезпечує точність, повноту та вагомість виконаної роботи;
- обґрунтовує зроблені висновки;
- сприяє процесу перевірки;
- фіксує досягнення цілей завдань;
- є підґрунтям для програм покращення довіри.

2.5.3 Як правило, до початку роботи фахівці повинні встановити попередню програму перевірки. Необхідно документально оформити цю програму аудиту таким чином, щоб вона дозволяла фахівцям фіксувати виконану аудиторську роботу та визначати роботу, яка ще підлягає виконанню. Під час виконання роботи фахівці повинні оцінювати адекватність програми аудиту, ґрунтуючись на інформації, зібраній під час роботи над завданнями з аудиту. Якщо фахівці встановлюють недостатність запланованих процедур, вони повинні відповідно змінити програму аудиту.

2.5.4 Ефективність та нагляд необхідно документально оформляти у робочій документації завдань з аудиту. Опис і зміст робочої документації завдань з аудиту можуть різнитися залежно від обставин окремого завдання з аудиту. Однак, керівництво аудиту та підтвердження довіри до ІС повинно детально описувати обмежену кількість стандартних зразків робочої документації для різних типів завдань з аудиту. Стандартна робоча документація підвищує ефективність завдань з аудиту та контролю. Окрім того, керівництво аудиту та підтвердження довіри до ІС повинно визначити медіа-носії, які будуть використовуватися, а також процедури зберігання робочої документації.

2.5.5 Фахівці повинні забезпечити своєчасне оформлення документації про виконану роботу. Необхідно отримати всю інформацію та докази, необхідні для формування висновків або професійних суджень, до дати опублікування аудиторського звіту. Робоча документація завдань з аудиту повинна містити дати її підготовки і перевірки.

2.5.6 Робоча документація завдань з аудиту є власністю організації. Керівництво аудиту та підтвердження довіри до ІС контролює її і санкціонує доступ повноважного персоналу до неї. Вище виконавче керівництво та особи, відповідальні за корпоративне управління, затверджують запити зовнішніх аудиторів щодо надання доступу до робочої документації завдань з аудиту. Запити щодо надання доступу стороннім особам, які не є зовнішніми аудиторами, повинні затверджуватися вищим виконавчим керівництвом та особами, відповідальними за корпоративне управління, а також рекомендуватися юристами.

2.6 Отримані дані та висновки

2.6.1 Згідно з параграфом 2.4.5 фахівці повинні аналізувати зібрані докази та інформацію. Значущі відхилення від очікувань необхідно описувати в отриманих даних. Фахівці повинні підтверджувати такі дані в організації, що підлягає аудиту, а також описувати їх вплив на інші аспекти контрольного середовища.

2.6.2 Фахівці можуть пропонувати корегуючи заходи, але ніколи не вживати їх. Якщо організація, що підлягає аудиту, вживає вказані у початкових даних корегуючи заходи, що виправляють

2203 Ефективність і нагляд (продовження)

2.6 Отримані дані та висновки (продовження)

недоліки, до завершення завдань з аудиту, фахівці повинні описати такі корегуючи заходи у своїй документації.

2.6.3 Фахівці повинні робити висновки щодо отриманих даних та оцінювати їх вплив на цілі аудиту. Висновки формуються згідно з початковими даними. Якщо було вжито корегуючи заходи, можна сформулювати додаток до висновків, що пояснює такі корегуючи заходи та їх вплив на початкові висновки.

2.6.4 Усі сформульовані висновки, незалежно від досягнення цілей аудиту, необхідно документально оформляти у звіті про завдання з аудиту. Детальні вказівки щодо звітування наведено у Стандарті 1401 «Звітування» та в Настанові 2401 «Звітування».

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами

3.2 Зв'язок із процесами COBIT 5

3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

• найбільш придатні стандарти ISACA, які безпосередньо стосуються цієї настанови ;

• положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1005 Належна професійна ретельність	Фахівці з аудиту та підтвердження довіри до ІС повинні проявляти належну професійну ретельність, у тому числі дотримуватись діючих професійних стандартів аудиту при плануванні, виконанні та звітуванні за результатами завдань.
1006 Професійність	Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні колективно володіти необхідними навичками і проявляти професійність при виконанні завдань з аудиту та підтвердження довіри до ІС, а також бути професійно компетентними для здійснення роботи. Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні мати достатні знання про об'єкт перевірки.
1201 Планування завдань	Фахівці з аудиту та підтвердження довіри до ІС повинні планувати кожне завдання з аудиту та підтвердження довіри до ІС таким чином, щоб воно відповідало: • цілі (цілям), обсягу, часовим рамкам та запланованим результатам; • діючим законам та професійним аудиторським стандартам; • застосуванню, за необхідності, ризик-орієнтованого підходу; • питанням, що виникають у зв'язку зі специфікою завдань; • вимогам до документації та звітності. Фахівці з аудиту та підтвердження довіри до ІС повинні розробляти та документально оформляти проектний план завдань з аудиту та підтвердження довіри до ІС, що описує: • характер, цілі та часові рамки завдань, а також потреби у ресурсах; • терміни проведення та обсяг аудиторських процедур, необхідних для виконання завдань.

2203 Ефективність і нагляд (продовження)

3.1 Зв'язок зі стандартами (продовження)

Назва стандарту	Відповідні положення стандарту
1203 Ефективність і нагляд	Фахівці з аудиту та підтвердження довіри до ІС повинні здійснювати роботу за узгодженим графіком у відповідності до затвердженого плану аудиту ІС, щоб охопити виявлені ризики. Фахівці з аудиту та підтвердження довіри до ІС повинні забезпечити контроль за роботою аудиторського персоналу, який вони курують, щоб досягти аудиторських цілей у відповідності до діючих професійних аудиторських стандартів. Фахівці з аудиту та підтвердження довіри до ІС повинні братися за виконання тільки таких задач, які можна завершити за допомогою уже наявних знань і навичок, або якщо вони мають обґрунтовані очікування щодо набуття таких навичок у процесі роботи чи виконання задач під наглядом. Для досягнення аудиторських цілей фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази. Аудиторські результати та висновки повинні супроводжуватись відповідним аналізом та тлумаченням таких доказів. Фахівці з аудиту та підтвердження довіри до ІС повинні документально оформляти процес аудиту, описуючи аудиторську роботу та аудиторські докази, що обґрунтовують результати та висновки. Фахівці з аудиту та підтвердження довіри до ІС повинні визначати та робити висновки щодо результатів.
1205 Докази	Фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази, щоб зробити обґрунтовані висновки, на які спиратимуться результати завдань. Фахівці з аудиту та підтвердження довіри до ІС повинні оцінювати достатність отриманих доказів для обґрунтування висновків та досягнення цілей завдань.
1401 Звітування	Фахівці з аудиту та підтвердження довіри до ІС повинні звітувати про результати виконаних завдань, включаючи: • ідентифікацію організації, припустимого одержувача та будь-які обмеження щодо змісту та розповсюдження; • обсяг, цілі та період виконання завдань, а також характер, визначення терміну проведення та обсягу роботи, що підлягає здійсненню; • результати, висновки та рекомендації; • будь-які кваліфікації фахівців з аудиту та підтвердження довіри до ІС чи обмеження обсягу робіт, що стосуються виконання завдань; • підпис, дату та розповсюдження згідно з умовами статуту аудиту та контракту. Фахівці з аудиту та підтвердження довіри до ІС повинні гарантувати, що наведені в аудиторському звіті результати ґрунтуються на достатніх та відповідних аудиторських доказах.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
• Процеси COBIT 5
• Цілі процесів COBIT 5
Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
APO07 Управляти персоналом	Оптимізувати можливості персоналу таким чином, щоб вони відповідали цілям організації.
APO08 Управляти взаємовідносинами	Удосконалювати результати, збільшувати впевненість, закріпляти довіру до IT та забезпечити ефективне використання ресурсів.
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.

2203 Ефективність і нагляд (продовження)

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:

- у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Ефективність дизайну	Якщо контролі компанії функціонують так, як визначено особами, що володіють необхідними повноваженнями і професійною компетентністю для ефективного здійснення таких контролів, вони відповідають цілям контролів компанії і можуть ефективно запобігати виникненню або виявляти помилки чи шахрайство, які можуть призвести до значних недостовірностей у фінансових звітах, вони вважаються ефективними з точки зору їх дизайну. Джерело: PCAOB[11], Аудиторський стандарт № 5, 2007 р.
Ефективність функціонування	Якщо контролі функціонують так, як вони були розроблені, а особи, що виконують їх, володіють необхідними повноваженнями і професійною компетентністю для ефективного здійснення таких контролів, вони вважаються ефективно функціонуючими. Джерело: PCAOB, Аудиторський стандарт № 5, 2007 р.
Контрольне середовище	Позиція та дії керівної ради і керівництва стосовно значущості контролю в організації. Контрольне середовище забезпечує упорядкованість і структуру для досягнення головних цілей системи внутрішніх контролів. Контрольне середовище включає наступні елементи: • чесність та етичні цінності; • філософію та стиль управління; • організаційну структуру; • делегування повноважень та обов'язків; • політики та процедури управління персоналом; • професійну компетентність персоналу. Джерело: Міжнародні стандарти професійної практики внутрішнього аудиту, 2010 р.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

[11] PCAOB (Public Company Accounting Oversight Board) – Комітет з нагляду за звітністю відкритих акціонерних компаній

2204 Суттєвість

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови полягає у чіткому визначенні концепції суттєвості для фахівців з аудиту та підтвердження довіри до ІС та у поясненні чіткої відмінності від концепції суттєвості для фахівців з фінансового аудиту та підтвердження довіри.

1.1.2 Ця настанова сприяє оцінюванню фахівцями з аудиту та підтвердження довіри до ІС суттєвості об'єкта перевірки та розгляду суттєвості з врахуванням контролів і питань, що підлягають звітуванню.

1.1.3 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1201 Планування завдань
1.2.2 Стандарт 1202 Оцінювання ризиків при плануванні
1.2.3 Стандарт 1204 Суттєвість
1.2.4 Стандарт 1207 Невідповідності та незаконні дії

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані зі завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Порівняння завдань з аудиту ІС та фінансових завдань з аудиту
2.2 Оцінювання суттєвості об'єкта перевірки
2.3 Суттєвість і контролі
2.4 Суттєвість і питання, що підлягають звітуванню

2.1 Порівняння завдань з аудиту ІС та фінансових завдань з аудиту

2.1.1 Фахівці у сфері ІС потребують інших критеріїв для виміру суттєвості у порівнянні з їх колегами, які працюють над фінансовими завданнями з аудиту. Фахівці у сфері фінансів, як правило, вимірюють суттєвість у грошовій формі, оскільки вони вимірюють і звітують про те, що піддають аудиту, також у грошовій формі. Фахівці, що займаються ІС, як правило, займаються аудитом нефінансових складових, наприклад, контролів розробки та внесення змін до програм, контролів фізичного та логічного доступів, а також контролів комп'ютерних операцій на різноманітних системах. Таким чином, фахівцям у сфері ІС можуть бути потрібні настанови щодо оцінювання суттєвості для ефективного планування їхніх аудиторських завдань, зосередження їхніх зусиль на сферах підвищеного ризику, а також оцінювання серйозності виявлених помилок і вразливих місць.

2.2 Оцінювання суттєвості об'єкта перевірки

2.2.1 Оцінювання суттєвості – питання професійних суджень. Воно ґрунтується на розгляді реального та / або потенційного впливу на здатність організації досягати її бізнес-цілей за умови існування помилок, упущень, невідповідностей та незаконних дій, які можуть виникати внаслідок вразливих місць контролів у сфері, що підлягає аудиту. Якщо при проведенні аудиту ІС цілі аудиту ІС стосуються систем або операцій, пов'язаних з обробкою фінансових транзакцій, необхідно розглядати таке вимірювання суттєвості, яке здійснюється фахівцями у сфері фінансів.

2.2.2 Для оцінювання суттєвості фахівці повинні класифікувати інформаційні активи, враховуючи:

2204 Суттєвість (продовження)

2.2 Оцінювання суттєвості об'єкта перевірки (продовження)

- їх конфіденційність, доступність і цілісність;
- правила доступу до керування привілеями;
- ступінь важливості та ризиків для бізнесу;
- відповідність законам і нормативним документам.

Таке оцінювання повинно розглядати:

- характер оброблених даних та інформації, що зберігаються;
- технічне забезпечення ІС;
- архітектуру та програмне забезпечення ІС (програми та операційні системи);
- мережеву інфраструктуру ІС;
- операції ІС;
- середовища промислової експлуатації, розробки і тестування;
- діючі закони і нормативні документи.

2.2.3 Детальніші зразки факторів, які можна розглядати для оцінювання суттєвості:

- важливість бізнес-процесів, що підтримуються системами чи операціями;
- важливість інформаційних баз даних, що підтримуються системами чи операціями;
- кількість і типи розроблених програм;
- кількість користувачів інформаційних систем;
- кількість керівників і директорів, які працюють з інформаційними системами, класифікованих згідно з привілеями;
- критичність мережевих комунікацій, що підтримуються системами чи операціями;
- вартість систем чи операцій (технічного та програмного забезпечення, роботи персоналу, послуг, що надаються третіми особами, накладних витрат або будь-якого їх поєднання);
- потенційна вартість помилок (наприклад, пов'язаних із втраченим збутом, гарантійними вимогами, безповоротними витратами на розробку, витратами на рекламу з метою попередження, витратами на усунення помилок, витратами на охорону здоров'я та безпеку, надвисокими витратами на виробництво, сильними втратами тощо);
- вартість втрати критичної та важливої інформації, враховуючи грошові та часові витрати на її відтворення, а також шкоду репутації та іміджу;
- кількість доступів / транзакцій / запитів, що обробляються за певний період;
- характер, часові рамки та обсяг підготованих звітів і файлів, що підтримуються;
- характер і кількість оброблених матеріалів (наприклад, динаміка товарно-матеріальних запасів без зазначення вартості);
- вимоги договорів про рівень обслуговування і розміри потенційних штрафів;
- штрафи за невідповідність законодавчим, регуляторним і контрактним вимогам;
- штрафи за невідповідність медичним та екологічним вимогам, а також вимогам до безпеки;
- певні визначення або фактори суттєвості, що надаються законодавчими або регуляторним органами;
- передача діяльності, пов'язаної з IT, третім сторонам, що призводить до значущих змін стосовно відповідності регуляторним вимогам, наприклад, конфіденційності та захисту даних, правил контролю торговельної діяльності, фінансових вимог тощо.

2.2.4 Для належного зменшення ризиків аудиту необхідно визначати предметні сфери підвищеної важливості, розширюючи перевірку контролів (зменшуючи ризики системи контролю) та / або розширюючи процедури перевірки на суттєвість (зменшуючи ризики невиявлення помилок).

2.2.5 Фахівці повинні здійснювати повторне оцінювання встановленої суттєвості, якщо вони звертають увагу на зміни, зокрема обставини чи додаткову інформацію, що можуть впливати на суттєвість систем або операцій. Найбільш розповсюджені ситуації, в яких такі зміни можуть мати місце:

- суттєвість була визначена на ранній стадії, ґрунтуючись на оцінках або попередній інформації, які значно різняться від реальної ситуації;
- події або зміни обставин встановленої суттєвості значним чином впливають на здатність організації досягати своїх бізнес-цілей.

2.3 Суттєвість і контролі

2.3.1 Для досягнення цілей аудиту фахівці повинні визначати відповідні цілі контролів, а також те, що підлягає перевірці, враховуючи рівень толерантності до ризиків. З огляду на певні цілі контролів, контроль чи група контролів вважаються значними, якщо їх відсутність призводить до нездатності забезпечити достатню впевненість у досягненні цілей контролів.

2.3.2 Фахівці повинні враховувати суттєвість при визначенні характеру, часових рамок та обсягу аудиторських процедур, що застосовуються для перевірки контролю чи групи контролів. Для

2204 Суттєвість (продовження)

2.3 Суттєвість і контролі (продовження)

зменшення аудиторських ризиків значні контролі необхідно перевіряти ретельніше, частіше та обширніше, ніж незначні контролі.

2.3.3 Оцінюючи суттєвість, фахівці повинні враховувати:
- рівень помилок, прийнятний для керівництва, фахівців, відповідних регуляторних органів та інших зацікавлених сторін;
- можливість виникнення сукупного ефекту багатьох незначних помилок або недоліків і, відповідно, їх переростання у значні.

2.3.4 До початку роботи над завданнями з аудиту на місцях фахівці повинні отримати затвердження відповідними зацікавленими сторонами розкриття будь-яких існуючих суттєвих недоліків в організації, про які знають останні.

2.3.5 Якщо фахівці виявляють проблему порушення контролів, вони повинні оцінювати її вплив на загальні аудиторські висновки або професійну думку. Оцінюючи такий вплив, фахівці повинні враховувати різні аспекти настання такої проблеми порушення контролів, включаючи:
- масштаб;
- характер;
- особливі обставини.

2.3.6 Перевіряючи значні контролі, фахівці повинні оцінювати вплив компенсуючи контролів з метою мінімізації ризиків, пов'язаних з виявленою проблемою порушення контролів.
Така проблема порушення контролів повинна класифікуватися наступним чином:
- суттєвий недолік за умови неефективності компенсуючих контролів;
- значне порушення за умови часткової ефективності контролів відшкодувань;
- незначне порушення за умови зменшення контролів відшкодувань до прийнятного рівня.

2.3.7 Численні помилки або втрата контролю можуть призвести до сукупного ефекту, який повинні враховувати фахівці при визначення загальної суттєвості проблеми порушення контролів.

2.3.8 Фахівці повинні визначати, чи будь-яка із проблем порушення загальних контролів ІТ є значною. Значущість таких порушених загальних контролів ІТ необхідно оцінювати, враховуючи їхній вплив на контролі прикладних програм, тобто ефективність пов'язаних з ними контролів прикладних програм. Якщо недоліки прикладних програм викликані загальними контролями ІТ, то вони є значними. Наприклад, якщо програмні розрахунки податків є значною мірою помилковими внаслідок слабких контролів щодо змінення податкових таблиць, програмні контролі (розрахунки) і загальні контролі (контроль змін) є досить слабкими.

2.3.9 Фахівці повинні оцінювати порушення загальних контролів ІТ, враховуючи їх вплив на контролі прикладних програм, у сукупності з іншими проблемами порушення контролів. Наприклад, рішення керівництва не виправляти загальну проблему порушення контролів ІТ та пов'язані з ним впливи на контрольне середовище у сукупності з іншими проблемами порушення контролів, які впливають на контрольне середовище, можуть призвести до значної проблеми.

2.4 Суттєвість і питання, що підлягають звітуванню

2.4.1 При визначенні того, про які результати, висновки і рекомендації необхідно звітувати, фахівці повинні враховувати як суттєвість усіх виявлених помилок, так і суттєвість помилок, які можуть виникнути внаслідок вразливих місць контролів.

2.4.2 Якщо завдання з аудиту полягає у наданні керівництву впевненості щодо контролів ІС, у некваліфікованому висновку щодо адекватності контролів необхідно вказати, що при досягненні цілей контролів за умови відсутності будь-яких значних вразливих місць контролів діючі контролі відповідають загальноприйнятим.

2.4.3 Вразливі місця контролів вважаються значними і, відповідно, про них необхідно звітувати, якщо відсутність контролів може призвести до неможливості забезпечити достатню впевненість у досягненні цілей контролів. Якщо при виконанні аудиторських завдань фахівці визначають значні вразливі місця контролів, вони повинні розглядати опублікування кваліфікованого або несприятливого висновку про цілі аудиту.

2.4.4 Залежно від цілей завдань з аудиту фахівці повинні розглядати звітування керівництву про вразливі місця, що не є значними, особливо якщо вартість посилення контролів є невисокою. Окрім того, фахівці можуть рекомендувати способи усунення виявлених вразливих місць.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами
3.2 Зв'язок із процесами COBIT 5
3.3 Інші настанови

2204 Суттєвість (продовження)

3.1 Зв'язок зі стандартами

Таблиця розглядає:
- найбільш придатні стандарти ISACA, які безпосередньо стосуються цієї настанови;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1201 Планування завдань	Фахівці з аудиту та підтвердження довіри до ІС повинні розробляти та документально оформляти проектний план завдань з аудиту та підтвердження довіри до ІС, що описує: • характер, цілі та часові рамки завдань, а також потреби у ресурсах; • терміни проведення та обсяг аудиторських процедур, необхідних для виконання завдань.
1202 Оцінювання ризиків при плануванні	При плануванні індивідуальних завдань фахівці з аудиту та підтвердження довіри до ІС повинні визначати та оцінювати ризики, пов'язані зі сферою, що перевіряється. Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики, пов'язані з об'єктом перевірки, аудиторські ризики та інші відповідні ризики для організації.
1204 Суттєвість	При плануванні завдань фахівці з аудиту та підтвердження довіри до ІС повинні враховувати потенційні вразливі місця та відсутність контролів, а також те, чи такі вразливі місця та відсутність контролів можуть призвести до значного порушення чи суттєвого недоліку. При визначенні характеру, часових рамок та обсягу аудиторських процедур фахівці з аудиту та підтвердження довіри до ІС повинні враховувати аудиторську суттєвість та її зв'язок з аудиторськими ризиками. Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати сукупний ефект незначного браку контролів та вразливих місць, а також те, чи така відсутність контролів може перерости у значне порушення чи суттєвий недолік. У своїх звітах фахівці з аудиту та підтвердження довіри до ІС повинні розкривати наступне: • відсутність контролів чи їх неефективність; • значущість проблеми порушення контролів; • ймовірність того, що такі вразливі місця призведуть до значного порушення чи суттєвого недоліку.
1207 Невідповідності та незаконні дії	При виконанні завдань фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики існування невідповідностей та незаконних дій. При виконанні завдань фахівці з аудиту та підтвердження довіри до ІС повинні дотримуватись позиції професійного скептицизму. Фахівці з аудиту та підтвердження довіри до ІС повинні документально оформляти та вчасно звітувати перед відповідними особами про будь-які значні невідповідності чи незаконні дії.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
- Процеси COBIT 5
- Цілі процесів COBIT 5

Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
EDM03 Забезпечувати оптимізацію ризиків	Забезпечити, щоб ризики організації, пов'язані з ІТ, не перевищували рівень її схильності та піддатливості ризикам, вплив ризиків, пов'язаних з ІТ, на вартість організації визначений і контролюється, а потенціал відхилень, пов'язаних з невідповідностями, мінімізований.

2204 Суттєвість (продовження)

3.2 Зв'язок із процесами COBIT 5 (продовження)

Процес COBIT 5	Мета процесу
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:

- у колег, які працюють в їхній або інших організаціях, наприклад, через професійні асоціації або професійні групи у соціальних медіа;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Значне порушення	Порушення або поєднання порушень внутрішніх контролів, які є менш серйозними, ніж суттєвий недолік, та все ж є досить важливими, щоб привернути увагу осіб, відповідальних за нагляд. **Примітка.** Суттєвий недолік є значним порушенням або сукупністю значних порушень, за яких існує вища ніж значна ймовірність, що небажані події не будуть попередженні чи виявлені.
Ризик аудиту	Ризик дійти до хибного висновку ґрунтуючись на результатах аудиту. Є три складових ризику аудиту: • ризик системи контролю; • ризик не виявлення помилок; • ризик, притаманний організації.
Суттєвий недолік	Порушення чи поєднання порушень внутрішнього контролю, за яких існує значна ймовірність, що суттєва недостовірність не буде вчасно попереджена чи виявлена. Недолік контролю вважається суттєвим, якщо відсутність контролів призводить до неможливості забезпечити достатню довіру до об'єкту контролю, якої він має відповідати. Недолік, який класифікується як суттєвий, означає, що: • відсутність контролів та / або їх невикористання та / або неадекватність; • погіршення гарантоване. Існує зворотній зв'язок між суттєвістю та рівнем ризиків аудиту, прийнятних для фахівця з аудиту та підтвердження довіри до ІС, тобто чим вищий рівень суттєвості, тим нижча вірогідність виникнення ризиків аудиту, і навпаки.
Суттєвість	Аудиторська концепція важливості елемента інформації, враховуючи її вплив чи наслідки на функціонування об'єкта перевірки в цілому. Вираження відносної значущості чи важливості окремого питання в контексті організації в цілому.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2205 Докази

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови полягає у наданні фахівцям з аудиту та підтвердження довіри до ІС вказівок щодо отримання достатніх і відповідних доказів, оцінювання отриманих доказів і підготовки належної аудиторської документації.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1203 Ефективність і нагляд
1.2.2 Стандарт 1205 Докази
1.2.3 Стандарт 1206 Залучення інших експертів

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані зі завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Типи доказів
2.2 Отримання доказів
2.3 Оцінювання доказів
2.4 Підготовка аудиторської документації

2.1 Типи доказів

2.1.1 При плануванні та виконанні завдань фахівці повинні враховувати типи доказів, які необхідно зібрати, їх застосування для досягнення цілей завдань, а також різні рівні їх надійності. Різні типи доказів, застосування яких повинні враховувати фахівці:
- досліджені процеси та існування фізичних складових;
- документальні докази;
- звернення;
- аналіз.

2.1.2 Досліджені процеси та існування фізичних складових може стосуватися спостереження за діяльністю, майном та функціями ІС, як, наприклад:
- системи відстеження мережевої безпеки в дії;
- інвентаризації засобів у місцях їх зберігання за межами організації.

2.1.3 Документальні докази, зафіксовані на папері або іншим засобом, є, наприклад:
- письмовими політиками чи процедурами;
- результатами витягу даних;
- записами транзакцій;
- списками програм;
- іншими документами і записами, створеними в рамках звичайної діяльності.

2.1.4 Письмові та усні звернення осіб, що піддаються аудиту, можуть бути:
- письмовими заявами керівництва, наприклад, зверненнями щодо існування та ефективності внутрішніх контролів або планів реалізації нових фінансових систем;
- усними зверненнями щодо роботи процесу або плану подальшої роботи керівництва над заходами, пов'язаними з програмою усвідомлення важливості безпеки.

2205 Докази (продовження)

2.1 Типи доказів (продовження)

2.1.5 Результати аналізу інформації шляхом порівняння, моделювання, підрахунку та обґрунтування також можна застосовувати як докази, наприклад:
- порівняння цільових орієнтирів діяльності ІС із цільовими орієнтирами інших організацій або минулих періодів;
- порівняння коефіцієнта помилок різних програм, транзакцій та користувачів;
- повторне здійснення процесів чи контролів.

2.2 Отримання доказів

2.2.1 Для досягнення обґрунтованих аудиторських висновків фахівці повинні отримати достатні та відповідні докази, включаючи:
- здійснені процедури;
- результати здійснених процедур;
- вихідну документацію (в електронному чи паперовому форматі), записи та підтверджуючу інформацію для обґрунтування завдань з аудиту;
- документацію про виконання роботи у відповідності до діючих законів, нормативних документів і політик.

2.2.2 Якщо докази, які є усними зверненнями, вирішальні для формування професійних суджень чи аудиторського висновку, фахівці повинні отримати підтвердження таких звернень у письмовій чи електронній формі (наприклад, електронною поштою). Фахівці також повинні розглядати альтернативні докази з метою обґрунтування таких звернень і забезпечення їх надійності.

2.2.3 При зборі доказів фахівці повинні враховувати наступне:
- час, зусилля та витрати на отримання доказів, враховуючи достатність таких доказів для зменшення ризиків аудиту;
- значущість об'єкта оцінювання та аудиторських процедур, для яких необхідні такі докази при досягненні цілей аудиту та зменшенні ризиків аудиту;
- неможливість повного чи часткового отримання електронних доказів через деякий проміжок часу.

2.2.4 Процедури збору доказів різняться залежно від характеристик інформаційних систем, що підлягають аудиту, часових рамок аудиту, його обсягу та цілей, а також професійних суджень. Докази можуть збиратися із застосуванням ручних аудиторських процедур, CAATs[12] або поєднання цих процедур. Фахівці повинні обирати найбільш відповідну процедуру, враховуючи цілі аудиту ІС. Повинні розглядатися наступні процедури:
- **опитування та підтвердження** (процес отримання інформації від досвідчених осіб, знайомих з об'єктом перевірки, які не є членами організації, що підлягає аудиту; ця процедура може застосовувати як офіційні письмові, так і неофіційні усні запити);
- **спостереження** (спостереження за процедурами чи процесами, що здійснюються особами, які, як правило, відповідають за їх здійснення, або спостереження за фізичними складовими, як, наприклад, за майном, комп'ютерним оснащенням або налаштуваннями та конфігураціями інформаційних систем; такий тип доказів обмежується часом здійснення спостереження; фахівці повинні враховувати те, що спостереження за виконанням процедур чи процесів може впливати на якість їх виконання);
- **перевірка** (перевірка внутрішньої або зовнішньої документації та записів; складові, що піддаються перевірці, можуть бути в паперовому чи електронному форматі; окрім того, можуть перевірятися і фізичні об'єкти);
- **аналітичні процедури** (оцінювання фінансових або нефінансових даних шляхом дослідження можливих взаємозв'язків даних або між даними та іншою відповідною інформацією; окрім того, можуть досліджуватися коливання, тенденції та суперечливі взаємозв'язки);
- **перерахунки / підрахунки** (процес перевірки арифметичної та математичної точності документації та записів вручну або за допомогою CAATs);
- **повторне проведення** (незалежне здійснення процедур та / або контролів, які спершу виконувалися інформаційною системою або самою організацією);
- **інші загальноприйняті методи** (інші загальноприйняті процедури, яким можуть слідувати фахівці при зборі достатніх і відповідних доказів; наприклад, фахівці можуть виконувати завдання з прикладної соціології, бути анонімними учасниками або виконувати перевірку шляхом етичного проникнення).

[12] CAATs (computer-assisted audit techniques) – комп'ютеризовані методики аудиту

2205 Докази (продовження)

2.2 Отримання доказів (продовження)

2.2.5 При зборі доказів фахівці повинні враховувати незалежність і кваліфікації осіб, що надають аудиторські докази. Наприклад, підтверджуючі аудиторські докази від незалежної третьої особи можуть бути надійнішими, ніж аудиторські докази від організації, що підлягає аудиту. Фізичні аудиторські докази, як правило, надійніші, ніж звернення осіб.

2.2.6 У випадку існування ймовірності того, що зібрані докази можуть використовуватися у судовій справі, фахівці повинні порадитися з відповідним юрист-консультантом для визначення особливих вимог, що можуть впливати на необхідний спосіб збору, подачі та розкриття доказів.

2.2.7 Якщо фахівці не можуть отримати достатні аудиторські докази, наприклад, якщо якісь особи чи керівництво відмовляються надати достатні та відповідні докази, необхідні для досягнення цілей аудиту ІС, фахівці повинні повідомити про таку ситуацію керівництво аудиту та, за необхідності, осіб, відповідальних за корпоративне управління, у відповідності до процедур, встановлених аудиторською організацією. Обмеження обсягу та досягнення цілей аудиту також необхідно розкривати у звітах про результати аудиту.

2.2.8 Фахівці повинні зберігати докази після завершення аудиторської роботи для забезпечення:
- їх доступності на період та у форматі, що відповідає політиці організації щодо аудиту, а також відповідним професійним стандартам, законам і нормативним документам;
- їх захисту від несанкціонованого розкриття та зміни протягом підготовки та зберігання;
- їх належного знищення після завершення періоду зберігання.

2.3 Оцінювання доказів

2.3.1 Докази є достатніми та відповідними, якщо вони обґрунтовують результати і висновки в рамках цілей аудиту. Якщо згідно із судженнями фахівців докази не відповідають цим критеріям, вони повинні отримати додаткові докази або здійснити додаткові процедури, щоб зменшити обмеження або невизначеність, пов'язані із доказами. Наприклад, список програм може не бути адекватним доказом, поки не будуть зібрані додаткові докази для підтвердження того, що він містить реальні програми, які застосовуються у виробничому процесі.

2.3.2 При оцінюванні надійності доказів, отриманих під час аудиту, фахівці повинні враховувати їх характеристики та властивості, як, наприклад, їх джерело, характер (наприклад, письмові, усні, візуальні, електронні), автентичність (наприклад, електронні та власноручні підписи, штампи часу / дати) і взаємозв'язок між доказами для надання підтверджуючих доказів з різних джерел. Загалом, надійність доказів різниться від низької до високої залежно від процедур отримання доказів, які можуть бути наступними:
- опитування та підтвердження;
- спостереження;
- перевірки;
- аналітичні процедури;
- перерахунки та підрахунки;
- повторне проведення.

У кожній із цих процедур надійність доказів загалом є вищою у випадку, якщо такі докази:
- є письмовими, а не усними зверненнями;
- отримані безпосередньо фахівцями, а не опосередковано установою, що підлягає аудиту;
- отримані з незалежних джерел;
- засвідчені незалежною стороною;
- зберігаються незалежною стороною.

2.3.3 Фахівці повинні враховувати період існування та доступності інформації при визначенні характеру, часових рамок та обсягу перевірки на суттєвість і, за необхідності, перевірки на відповідність. Наприклад, докази, оброблені за допомогою EDI[13], DIP[14] і таких динамічних систем, як, наприклад, електронна таблиця, можуть не витягнутися через деякий проміжок часу, якщо не контролювати зміни файлів або не архівувати їх. Політика організації щодо зберігання документації також може впливати на доступність останньої.

2.3.4 У випадку аудиту незалежною третьою стороною фахівці повинні враховувати виконання перевірки контролів, пов'язаних з об'єктом аудиту, а також рівень надійності результатів такої перевірки.

[13] EDI (electronic data interchange) – система електронного обміну даними

[14] DIP (document and image processing) – обробка документів і зображень

2205 Докази (продовження)

2.3 Оцінювання доказів (продовження)

2.3.5 Фахівці повинні отримати достатні та відповідні докази для того, щоб кваліфікована незалежна сторона могла знову здійснити таку перевірку та дійти тих самих результатів і висновків.

2.4 Підготовка аудиторської документації

2.4.1 При проведенні аудиту фахівці повинні готувати таку документацію, пов'язану з отриманими доказами, яка зберігатиметься та буде доступною протягом попередньо визначеного проміжку часу та у форматі, що відповідає політиці організації щодо аудиту, а також відповідним професійним стандартам, законам і нормативним документам.

2.4.2 Для встановлення загальної достатності та відповідності доказів з метою обґрунтування результатів і висновків у рамках цілей аудиту, а також для легкого отримання доказів членами групи, що займається аудитом ІС, або незалежною стороною докази, що отримуються під час аудиту, їх необхідно належним чином визначати, каталогізувати та зробити перехресні посилання .

2.4.3 Фахівці повинні забезпечити захист документації, пов'язаної з доказами, від несанкціонованого розкриття та зміни протягом її підготовки та зберігання.

2.4.4 Фахівці повинні належним чином знищити документацію, пов'язану з доказами, після завершення встановленого періоду її зберігання.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами

3.2 Зв'язок із процесами COBIT 5

3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA щодо аудиту та підтвердження довіри до ІС, які безпосередньо стосуються цієї настанови;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1203 Ефективність і нагляд	Для досягнення аудиторських цілей фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази. Аудиторські результати та висновки повинні супроводжуватись відповідним аналізом та тлумаченням таких доказів. Фахівці з аудиту та підтвердження довіри до ІС повинні документально оформляти процес аудиту, описуючи аудиторську роботу та аудиторські докази, що обґрунтовують результати та висновки.
1205 Докази	Фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази, щоб зробити обґрунтовані висновки, на які спиратимуться результати завдань. Фахівці з аудиту та підтвердження довіри до ІС повинні оцінювати достатність отриманих доказів для обґрунтування висновків та досягнення цілей завдань.
1206 Залучення інших експертів	Фахівці з аудиту та підтвердження довіри до ІС повинні застосовувати додаткові процедури перевірки для отримання достатніх та відповідних доказів, якщо їх не надає робота інших експертів.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:

- Процеси COBIT 5
- Цілі процесів COBIT 5

Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

2205 Докази (продовження)

3.2 Зв'язок із процесами COBIT 5 (продовження)

Процес COBIT 5	Мета процесу
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
- у колег, що працюють в організації;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- у професійних організаціях або медіа-групах;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Відповідні докази	Міра довіри до доказів.
Достатні докази	Міра кількості доказів; обґрунтовують усі суттєві питання щодо цілей та обсягу аудиту. Дивіться визначення терміну «докази».
Звернення	Підписана або усна заява керівництва, у якій фахівці повідомляються про те, що згідно з наявними даними певний факт (наприклад, процес, система, процедура чи політика), який зараз має або у майбутньому матиме місце, знаходиться або знаходитиметься у певному стані.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2206 Залучення інших експертів

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Ця настанова надає фахівцям з аудиту та підтвердження довіри до ІС вказівки щодо розгляду залучення інших експертів, а також сприяє аналізу їх адекватності, перевірці та оцінюванню їх роботи, визначенню необхідності здійснення додаткових процедур перевірки та формуванню професійних суджень про завдання з аудиту, враховуючи роботу, виконану іншими експертами.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1007 Твердження
1.2.2 Стандарт 1203 Ефективність і нагляд
1.2.3 Стандарт 1206 Залучення інших експертів

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані зі завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Розгляд залучення інших експертів
2.2 Аналіз адекватності інших експертів
2.3 Планування і перевірка роботи інших експертів
2.4 Оцінювання роботи інших експертів, які не є членами групи, що виконує завдання з аудиту
2.5 Додаткові процедури перевірки
2.6 Аудиторські оцінки та висновки

2.1 Розгляд залучення інших експертів

2.1.1 Якщо фахівці не мають компетенції, необхідної для виконання (частини) завдань з аудиту, вони повинні розглядати звернення до інших експертів, які володіють необхідними навичками.

2.1.2 Залучення інших експертів слід розглядати у випадку існування обмежень, які можуть погіршити якість аудиторської роботи, що підлягає виконанню, враховуючи потенційні загрози незалежності, наприклад, необхідність певних технічних знань у зв'язку з характером поставлених задач, брак аудиторських ресурсів і часові обмеження. Окрім того, залучення інших експертів необхідно розглядати, якщо воно покращить якість виконання завдань.

2.1.3 Фахівці повинні мати достатні знання роботи, яку вони виконують, щоб управляти нею і перевіряти її, але рівень їх знань не повинен обов'язково відповідати рівню знань експертів.

2.1.4 Фахівці повинні обґрунтовувати вибір певних експертів і залучати до роботи інших експертів за об'єктивними критеріями.

2.1.5 Фахівці повинні інформувати інших експертів і документально оформляти вимоги до їх роботи у контракті чи договорі до початку виконання завдань іншими експертами.

2.1.6 Якщо доступ інших експертів до записів або систем заборонений внутрішньою політикою організації, фахівці повинні визначати відповідний обсяг їх залучення та покладання на результати їх роботи.

2.1.7 За умови неможливості залучення необхідних експертів фахівці повинні документально

2206 Залучення інших експертів (продовження)

2.1 Розгляд залучення інших експертів (продовження)

оформляти вплив цього на досягнення цілей аудиту та включати відповідні задачі в план аудиту для управління ризиками аудиту. Якщо внаслідок цього ризики аудиту не піддаються управлінню, може виникнути необхідність відмови фахівців від виконання завдань з аудиту.

2.2 Аналіз адекватності інших експертів

2.2.1 Якщо завдання з аудиту включають залучення інших експертів, при плануванні роботи з аудиту ІС фахівці повинні враховувати їх адекватність, включаючи:
- оцінювання незалежності та об'єктивності інших експертів;
- оцінювання їх професійних кваліфікацій, компетенції, відповідного досвіду, ресурсів і процесів контролю довіри.

2.2.2 Фахівці повинні ретельно розглядати незалежність та об'єктивність інших експертів, залучаючи їх до роботи. Процеси вибору і призначення, статус в організації, лінії звітування і вплив їх рекомендацій на діяльність керівництва є типовими показниками незалежності та об'єктивності інших експертів.

2.3 Планування і перевірка роботи інших експертів

2.3.1 При плануванні роботи з аудиту ІС фахівці повинні розглядати діяльність інших експертів і їх вплив на цілі аудиту, включаючи:
- розуміння ними обсягу роботи, підходу, часових рамок і процесів контролю довіри;
- визначення рівня необхідної перевірки.

2.3.2 Фахівці повинні перевіряти, чи статут аудиту або контракт встановлюють право доступу до роботи інших експертів. Фахівці повинні мати доступ до всієї робочої та супровідної документації і звітів інших експертів, якщо це не створює суперечок з правової точки зору.

2.3.3 Характер, часові рамки та обсяг необхідних аудиторських доказів залежить від значущості та обсягу роботи інших експертів. У процесі планування фахівці повинні визначати рівень перевірки, необхідної для надання достатніх і відповідних аудиторських доказів та ефективного досягнення загальних цілей аудиту ІС. Фахівці повинні перевіряти остаточний варіант звітів, методології, аудиторські програми та робочу документацію інших експертів.

2.3.4 Перевіряючи робочу документацію інших експертів, фахівці повинні оцінювати належність планування, контролю, документального оформлення та перевірки їх роботи з метою визначення відповідності та достатності наданих ними аудиторських доказів, а також обсягу їх залучення та покладання на результати їх роботи. Таке оцінювання може включати повторну перевірку роботи інших експертів. Окрім того, необхідно оцінювати відповідність професійним стандартам. Загалом, фахівці повинні оцінювати, чи робота інших експертів є достатньо адекватною і повною для формування та документального оформлення ними висновків щодо поточних цілей аудиту ІС.

2.3.5 Фахівці повинні належним чином перевіряти остаточний варіант звітів інших експертів для підтвердження:
- відповідності обсягу, встановленого у статуті аудиту, поставлених задач і контракту;
- виявлення усіх значущих припущень, що застосовувалися іншими експертами;
- достатності обґрунтування доказами результатів і висновків, зазначених у звітах.

2.4 Оцінювання роботи інших експертів, які не є членами групи, що виконує завдання з аудиту

2.4.1 Сьогоднішні взаємозалежності клієнтів і постачальників щодо здійснення та передачі підрядникам на умовах аутсорсингу неголовної діяльності приводить до більш складного аудиторського середовища. Частини середовища, що підлягають аудиту, можуть перевірятися і контролюватися іншими незалежними функціями та організаціями. Таким чином, організація, що залучає підрядників на умовах аутсорсингу, отримує звіти від третіх сторін про контрольне середовище діяльності, яку виконують інші експерти. У деяких випадках це може зменшити потребу покриття всієї сфери аудиту ІС, навіть якщо фахівці не матимуть доступу до робочої та супровідної документації. У таких випадках фахівці повинні надавати свої професійні судження з обережністю.

2.4.2 Фахівці повинні оцінювати корисність і відповідність звітів інших експертів і враховувати усі значущі результати, про які звітують інші експерти. Обов'язком фахівців також є визначення того, чи можна вважати роботу інших експертів надійною і безпосередньо включати її або посилатися на неї у звіті. Окрім того, фахівці повинні оцінювати вплив результатів і висновків інших експертів

2206 Залучення інших експертів (продовження)

2.4 Оцінювання роботи інших експертів, які не є членами групи, що виконує завдання з аудиту (продовження)

на загальні цілі аудиту ІС і підтверджувати завершення усіх додаткових робіт, необхідних для досягнення цілей аудиту ІС. Керівництво повинно перевіряти та офіційно схвалювати усі твердження інших експертів. Детальні вказівки щодо цього питання наведено у Стандарті 1007 «Твердження».

2.5 Додаткові процедури перевірки

2.5.1 Ґрунтуючись на оцінюванні роботи інших експертів, фахівці повинні застосовувати додаткові процедури перевірки для отримання достатніх і відповідних аудиторських доказів у тих випадках, коли робота інших експертів не надає такі докази.

2.5.2 Фахівці також повинні розглядати необхідність здійснення додаткової перевірки роботи інших експертів.

2.6 Аудиторські оцінки та висновки

2.6.1 Фахівці несуть повну та одноосібну відповідальність за формування аудиторських оцінок і висновків. Фахівці повинні визначати достатність роботи, виконаної іншими експертами, для формування аудиторських оцінок і висновків.

2.6.2 Якщо здійснені додаткові процедури перевірки не надають достатніх і відповідних аудиторських доказів, фахівці повинні забезпечити формування відповідних аудиторських оцінок і висновків, зазначаючи, за необхідності, обмеження обсягу.

2.6.3 Судження та коментарі фахівців щодо прийнятності та відповідності звітів інших експертів необхідно включати у звіт про результати завдань з аудиту, якщо звіти інших експертів використовувалися при формуванні оцінок фахівців.

2.6.4 За необхідності, фахівці повинні розглядати обсяг виконання керівництвом рекомендацій інших експертів, включаючи оцінювання того, чи керівництво налаштоване на вирішення питань, виявлених іншими експертами, у відповідні часові рамки, а також поточний статус відповідних заходів.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами

3.2 Зв'язок із процесами COBIT 5

3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA щодо аудиту та підтвердження довіри до ІС, які безпосередньо стосуються цієї настанови;
- положення стандартів, які є найбільш придатні для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1007 Твердження	Фахівці з аудиту та підтвердження довіри до ІС повинні перевіряти твердження, на основі яких здійснюватиметься оцінювання об'єкта перевірки, для визначення того, чи такі твердження можна піддати аудиту, і чи є вони достатніми, обґрунтованими та відповідними.
1203 Ефективність і нагляд	Фахівці з аудиту та підтвердження довіри до ІС повинні братися за виконання тільки таких задач, які можна завершити за допомогою уже наявних знань та навичок, або якщо вони мають обґрунтовані очікування щодо набуття таких навичок у процесі роботи чи виконання задач під наглядом. Для досягнення аудиторських цілей фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази. Аудиторські результати та висновки повинні супроводжуватись відповідним аналізом та тлумаченням таких доказів.

2206 Залучення інших експертів (продовження)

3.1 Зв'язок зі стандартами (продовження)

Назва стандарту	Відповідні положення стандарту
1206 Залучення інших експертів	Фахівці з аудиту та підтвердження довіри до ІС повинні, за необхідності, розглядати можливість залучення інших експертів для виконання завдань. Фахівці з аудиту та підтвердження довіри до ІС повинні оцінювати та підтверджувати відповідність професійних кваліфікацій, компетенції, відповідного досвіду, ресурсів, незалежності та процесів контролю довіри до інших експертів до початку виконання завдань. У рамках виконання своїх завдань фахівці з аудиту та підтвердження довіри до ІС повинні визначати, переглядати та оцінювати роботу інших експертів, а також документально оформляти висновки щодо обсягу залучення таких експертів та покладання на результати їх роботи. Фахівці з аудиту та підтвердження довіри до ІС повинні визначати, чи є робота інших експертів, які не є членами групи, що виконує завдання, достатньо адекватною та вичерпною для досягнення поточних цілей завдань, а також чітко документально оформляти свої висновки. Фахівці з аудиту та підтвердження довіри до ІС повинні визначати, чи можна вважати роботу інших експертів надійною і безпосередньо включати її або посилатися на неї у звіті. Фахівці з аудиту та підтвердження довіри до ІС повинні застосовувати додаткові процедури перевірки для отримання достатніх та відповідних доказів, якщо їх не надає робота інших експертів. Фахівці з аудиту та підтвердження довіри до ІС повинні надавати відповідні аудиторські оцінки або висновки та включати в них будь-які обмеження обсягу робіт, якщо необхідні докази не можна отримати за допомогою додаткових процедур перевірки.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
• Процеси COBIT 5
• Цілі процесів COBIT 5
Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
• у колег, що працюють в організації;
• у керівництва;
• в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
• у професійних організаціях або медіа-групах;
• в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

2206 Залучення інших експертів (продовження)

4. Термінологія

Термін	Визначення
Інші експерти	Внутрішні та зовнішні по відношенню до організації, інші експерти можуть належить до: • аудиторів ІС з зовнішньої бухгалтерської фірми; • консультанти з питань управління; • експерти у предметній сфері завдання, призначені вищим виконавчим керівництвом компанії або групою.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2207 Невідповідності та незаконні дії

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови полягає у наданні фахівцям з аудиту та підтвердження довіри до ІС вказівок щодо того, як боротися з невідповідностями та незаконними діями.

1.1.2 Ця настанова описує обов'язки керівництва і фахівців з аудиту та підтвердження довіри до ІС щодо невідповідностей та незаконних дій. Окрім того, вона надає вказівки щодо того, як боротися з невідповідностями та незаконними діями при плануванні та здійсненні аудиторської роботи, а також описує передовий досвід внутрішнього та зовнішнього звітування щодо невідповідностей та незаконних дій.

1.1.3 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1005 Належна професійна ретельність
1.2.2 Стандарт 1201 Планування завдань
1.2.3 Стандарт 1202 Оцінювання ризиків при плануванні
1.2.4 Стандарт 1207 Невідповідності та незаконні дії
1.2.5 Стандарт 1401 Звітування

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані зі завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Невідповідності та незаконні дії
2.2 Обов'язки керівництва
2.3 Обов'язки фахівців
2.4 Невідповідності та незаконні дії при плануванні завдань
2.5 Розробка та перевірка процедур завдань
2.6 Реагування на невідповідності та незаконні дії
2.7 Внутрішнє звітування
2.8 Зовнішнє звітування

2.1 Невідповідності та незаконні дії

2.1.1 Невідповідності та незаконні дії можуть впливати безпосередньо на організацію різними (негативними) способами, як, наприклад, на її фінанси та репутацію, а також безпосередньо на ефективність і збереження співробітників. Таким чином, важливо, щоб організація мала механізми інформування, попередження та виявлення невідповідностей та незаконних дій для їх швидкого визначення. Невідповідності та незаконні дії частіше виникають в областях із відсутніми, слабо розробленими або не функціонуючими контролями.

2.1.2 Співробітники будь-якого рівня організації можуть призводити до виникнення невідповідностей і незаконних дій, включаючи, але не обмежуючись:
- шахрайством, що є будь-якою дією, пов'язаною з обманом, з метою отримання незаконної вигоди;

2207 Невідповідності та незаконні дії (продовження)

2.1 Невідповідності та незаконні дії (продовження)

- навмисним перекручуванням фактів з метою отримання незаконної вигоди або приховування невідповідностей і незаконних дій;
- діями, пов'язаними із недотриманням законів і нормативних документів, включаючи невідповідність систем ІТ діючим законам і нормативним документам;
- несанкціонованим розкриттям даних, які підпадають під закони про конфіденційність;
- діями, пов'язаними із недотриманням умов договорів і контрактів організації з третіми сторонами, наприклад, з банками, постачальниками, продавцями, постачальниками послуг і зацікавленими сторонами;
- маніпуляціями, фальсифікаціями, підробками або зміною записів і документів (в електронному чи паперовому форматі);
- приховуванням або замовчуванням впливу транзакцій у записах чи документах (в електронному чи паперовому форматі);
- неприйнятним або навмисним витоком конфіденційної інформації;
- фіксуванням транзакцій у фінансових або інших документах (в електронному чи паперовому форматі), яким бракує обґрунтованості та які є неправдивими (наприклад, фальшиві витрати, шахрайство з фондами заробітної плати, ухилення від сплати податків тощо);
- незаконним присвоєнням і нецільовим використанням коштів;
- приховуванням доходів або розтратою коштів, що є незаконним присвоєнням коштів до фіксування їх у фінансових документах організації;
- навмисними або ненавмисними діями, пов'язаними з порушенням права інтелектуальної власності, наприклад, авторського права, товарних знаків або патентів;
- наданням несанкціонованого доступу до інформації та систем;
- помилками у фінансовій або іншій документації, що виникають внаслідок несанкціонованого доступу до даних і систем.

2.1.3 Як правило, визначення незаконності певних дій ґрунтується на рекомендаціях інформованих експертів, компетентних у сфері юриспруденції, або на заключному рішенні суду загальної юрисдикції. Перш за все, фахівці повинні звертати увагу на вплив або потенційний вплив незаконних дій, незалежно від того, чи такі дії вважаються припустимими, чи є незаконними.

2.1.4 Не всі невідповідності вважаються шахрайськими діями. Визначення останніх залежить від правового визначення шахрайства у відповідній юрисдикції. Шахрайські невідповідності включають, але не обмежуються:

- навмисним обходом контролів з метою приховання шахрайства;
- несанкціонованим використанням активів або послуг;
- співучастю або сприянням у прихованні таких видів діяльності.

Приклади нешахрайських невідповідностей:

- навмисне порушення встановлених політик керівництва;
- навмисне порушення регуляторних вимог;
- навмисні недостовірності або упущення інформації стосовно сфери, яка підлягає аудиту, або організації в цілому;
- груба недбалість;
- ненавмисне вчинення незаконних дій.

2.2 Обов'язки керівництва

2.2.1 Забезпечення контролів для перешкоджання, попередження та виявлення невідповідностей і незаконних дій є перш за все обов'язком керівництва та керівної ради.

2.2.2 Як правило, керівництво застосовує наступні заходи для забезпечення достатньої впевненості у своєчасному перешкоджанні, попередженні та виявленні невідповідностей і незаконних дій:

- розробку, впровадження та підтримку систем внутрішніх контролів попередження та виявлення невідповідностей або незаконних дій; внутрішні контролі включають перегляд і затвердження операцій, а також процедури перевірки керівництва;
- політики і процедури управління поведінкою співробітників;
- відповідність процедурам підтвердження та відстеження ;
- розробку, застосування та підтримку відповідних систем звітування, фіксування та управління випадками, пов'язаними з невідповідностями або незаконними діями;
- політики і процедури управління відповідністю регуляторним вимогам.

2.2.3 Керівництво повинно інформувати фахівців про будь-які відомі йому невідповідності або незаконні дії, незалежно від того, чи вони є сумнівними, припустимими або доведеними, і про

2207 Невідповідності та незаконні дії (продовження)

2.2 Обов'язки керівництва (продовження)		сфери, на які впливають такі невідповідності або незаконні дії, а також про дії керівництва, якщо останні мають місце.
	2.2.4	У випадку існування сумнівних, припустимих або виявлених невідповідностей або незаконних дій керівництво повинно сприяти процесу їх дослідження та розслідування.
2.3 Обов'язки фахівців	2.3.1	Фахівці повинні розглядати визначення у статуті аудиту обов'язків керівництва та керівництва аудиту та підтвердження ІС щодо попередження, виявлення та звітування про невідповідності, щоб вони були чітко зрозумілими протягом виконання всієї аудиторської роботи. Якщо такі обов'язки вже документально оформлені у політиці організації або схожому документі, статут аудиту повинен містити положення відповідного змісту.
	2.3.2	Фахівці повинні розуміти, що контрольні механізми не можуть повністю виключити ймовірність виникнення невідповідностей або незаконних дій. Фахівці несуть відповідальність за оцінювання ризику виникнення невідповідностей або незаконних дій і впливу виявлених невідповідностей, а також за розробку та проведення перевірок, які відповідають характеру завдань з аудиту.
	2.3.3	Фахівці не несуть відповідальність за попередження та виявлення невідповідностей або незаконних дій. Виконання завдань з аудиту не може гарантувати виявлення невідповідностей. Навіть при належному плануванні та проведенні аудиту невідповідності можуть залишитися невизначеними, наприклад, у випадку існування таємної змови співробітників, таємної змови співробітників зі сторонніми особами або причетності керівництва до невідповідностей. Метою фахівців є визначення наявних, адекватних та ефективних контролів, яких дотримуються в організації.
	2.3.4	Якщо у фахівців є конкретна інформація про існування невідповідностей та незаконних дій, вони повинні звітувати про неї.
	2.3.5	Фахівці повинні інформувати керівництво та осіб, відповідальних за корпоративне управління, про виявлення ситуацій з підвищеним ризиком існування потенційних невідповідностей і незаконних дій, навіть якщо жодна не була виявлена.
	2.3.6	Фахівці повинні знати сферу, що підлягає аудиту, на такому рівні, щоб бути в змозі визначати фактори ризику, які сприяють виникненню невідповідностей і незаконних дій.
2.4 Невідповідності та незаконні дії при плануванні завдань	2.4.1	За допомогою відповідної методології фахівці повинні оцінювати ризик виникнення невідповідностей і незаконних дій, пов'язаний зі сферою, що підлягає аудиту. При підготовці такого оцінювання фахівці повинні враховувати наступні фактори: • характеристики організації, наприклад, корпоративну етику, організаційну структуру, адекватність нагляду, структури компенсацій та винагород, обсяг впливу на загальну результативність діяльності організації або напрямок діяльності організації; • історію організації, випадки виявлення невідповідностей у минулому та подальші заходи, пов'язані зі зменшенням або мінімізацією результатів таких невідповідностей; • нещодавні зміни керівництва, діяльності або ІС і поточний стратегічний напрямок діяльності організації; • вплив нових стратегічних партнерств; • типи активів або послуг, що надаються, та схильність до виникнення невідповідностей; • оцінювання ефективності відповідних контролів і вразливості організації до обходу або нехтування встановленими контролями; • діючі регуляторні або юридичні вимоги; • внутрішні політики, наприклад, політику корпоративного інформування, політику інсайдерської торгівлі та кодекс етики співробітників і керівництва; • взаємодію зацікавлених осіб та фінансові ринки; • кадровий потенціал; • конфіденційність і цілісність інформації, важливої для ринку; • результати попередніх аудитів; • галузеве та конкурентне середовище діяльності організації; • результати перевірок, здійснених за рамками обсягу аудиту, наприклад, результати, отримані від консультантів або груп контролю довіри, а також внаслідок певних досліджень керівництва; • результати, отримані в рамках щоденної діяльності; • наявність процесу оформлення документації та / або системи управління якістю; • технічну досконалість і складність інформаційних систем сфери, що підлягає аудиту;

2207 Невідповідності та незаконні дії (продовження)

2.4 Невідповідності та незаконні дії при плануванні завдань (продовження)

- наявність програмних систем власної розробки / обслуговування, пов'язаних з основними бізнес-системами, на противагу пакетному програмному забезпеченню;
- вплив незадоволення співробітників;
- потенційні скорочення персоналу, залучення підрядників, розформування підрозділів або реструктуризації;
- наявність активів, які можна легко незаконно присвоїти;
- низькі показники фінансової та / або операційної діяльності організації;
- відношення керівництва до етики;
- невідповідності та незаконні дії, що притаманні певній галузі або мали місце в аналогічній організації.

2.4.2 В рамках процесу планування та проведення оцінки ризиків фахівці повинні консультуватися з керівництвом і, за необхідності, отримувати його письмові звернення щодо:

- розуміння ним рівня ризику виникнення невідповідностей і незаконних дій в організації;
- відомої йому інформації про невідповідності та незаконні дії, які мали чи могли мати місце в організації чи проти неї;
- його відповідальності за розробку та впровадження внутрішніх контролів для запобігання невідповідностям і незаконним діям;
- відстеження та управління ризиком невідповідностей і незаконних дій;
- наявності діючих процесів, пов'язаних зі звітуванням відповідним зацікавленим сторонам про сумнівні, припустимі чи існуючі невідповідності або незаконні дії;
- відповідних національних і регіональних законів в юрисдикції діяльності організації, а також обсягу координування діяльності юридичного відділу із комітетом по ризиках та / або аудиторським комітетом.

2.5 Розробка та перевірка процедур завдань

2.5.1 Оскільки фахівці не несуть відповідальність за виявлення чи попередження незаконних дій і невідповідностей, вони повинні розробляти процедури для виконання завдань з аудиту, враховуючи рівень ризику виявлених незаконних дій і невідповідностей.

2.5.2 Фахівці повинні застосовувати результати оцінки ризиків при визначенні характеру, часових рамок та обсягу перевірок, необхідних для отримання достатніх аудиторських доказів при забезпеченні достатньої впевненості щодо виявлення:

- невідповідностей, які можуть значним чином впливати на сферу, що підлягає аудиту, чи організацію в цілому;
- вразливих місць контролів, які не даватимуть результатів при запобіганні чи визначенні значних невідповідностей;
- усіх значущих порушень при розробці чи функціонуванні внутрішніх контролів, які можуть потенційно впливати на здатність фіксувати, обробляти, підсумовувати та звітувати про дані діяльності.

2.5.3 Фахівці повинні перевіряти результати процедур завдань для визначення показників можливого виникнення невідповідностей або незаконних дій. CAATs можуть значним чином сприяти ефективному та дієвому виявленню невідповідностей і незаконних дій

2.5.4 При проведенні такої оцінки необхідно звірити фактори ризику, зазначені у параграфі 2.4.1, з реальними процедурами забезпечення достатньої впевненості у врахуванні усіх виявлених ризиків.

2.6 Реагування на невідповідності та незаконні дії

2.6.1 При виконанні завдань з аудиту фахівці можуть звернути увагу на ознаки існування невідповідностей або незаконних дій. Вони повинні враховувати потенційний вплив таких невідповідностей або незаконних дій на об'єкт перевірки завдань, цілі аудиту, звіти про завдання з аудиту та організацію.

2.6.2 Фахівці повинні проявляти професійний скептицизм. Ознаки наявності осіб, що призводять до виникнення невідповідностей і незаконних дій (які ще називають «сигналами ризику шахрайства» або «показниками ризику»):

- незастосування керівництвом контролів;
- незаконна або незрозуміла поведінка керівництва;
- систематичне перевиконання поставлених цілей;
- проблеми або затримки в отриманні необхідної інформації або доказів;
- операції, при здійсненні яких не дотримуються звичайні цикли затвердження;

2207 Невідповідності та незаконні дії (продовження)

2.6 Реагування на невідповідності та незаконні дії (продовження)

- підвищення активності певного клієнта;
- збільшення кількості скарг клієнтів;
- порушення контролю доступу до деяких програм чи користувачів.

Фахівці повинні бути особливо уважними при виявленні такої поведінки.

2.6.3 Якщо фахівці отримують інформацію щодо можливості існування невідповідностей і незаконних дій, після отримання вказівок від відповідних правових органів вони повинні розглядати наступні кроки:

- досягнення розуміння характеру таких дій;
- досягнення розуміння обставин їх виникнення;
- збір доказів їх виникнення (наприклад, листів, системних записів, комп'ютерних файлів, контрольних журналів, інформації від клієнтів і постачальників);
- визначення всіх осіб, причетних до таких дій;
- отримання достатньої кількості допоміжної інформації для оцінювання впливу таких дій;
- здійснення певних додаткових процедур для визначення впливу таких дій та існування інших невідповідностей або незаконних дій;
- документальне оформлення та збереження всіх доказів і виконаної роботи.

2.6.4 Фахівці повинні консультуватися з керівництвом аудиту для визначення подальших заходів, як, наприклад, звітування керівництву організації про «подію», передачу інформації про подальші дії внутрішнім експертам, що займаються дослідженням шахрайства, та / або звітування правоохоронним або регуляторним органам.

2.6.5 Якщо до невідповідностей причетний член керівництва, фахівці повинні переглянути надійність звернення до керівництва. Як правило, фахівці повинні працювати з таким рівнем керівництва, який є вищим від причетного до невідповідностей і незаконних дій.

2.7 Внутрішнє звітування

2.7.1 Фахівці повинні своєчасно звітувати (у письмовій або усній формі) відповідним особам в організації про виявлення невідповідностей і незаконних дій. Необхідно інформувати такий рівень керівництва, який є вищим від того, на якому могли мати місце невідповідності та незаконні дії. Окрім того, про невідповідності та незаконні дії необхідно звітувати особам, відповідальним за корпоративне управління організацією, наприклад, раді директорів, довірчим власникам, аудиторському комітету або рівнозначним органам, у тому числі про питання, які є незначущими стосовно їх фінансового впливу та ознак вразливих місць контролів.

Якщо фахівці допускають причетність усіх рівнів керівництва, про такі результати необхідно конфіденційно повідомити осіб, відповідальних за корпоративне управління організацією, наприклад, раду директорів, довірчих власників, аудиторський комітет або рівнозначні органи, згідно з діючими місцевими законами та нормативним документами, якщо правові органи не забороняють звітування таким особам.

2.7.2 Фахівці повинні застосовувати свої професійні судження при звітуванні про невідповідності та незаконні дії. Вони повинні обговорювати результати, а також характер, часові рамки та обсяг усіх подальших процедур з відповідним рівнем керівництва, який є щонайменше на один рівень вищим від причетних осіб. За таких обставин особливо важливо, щоб фахівці дотримувалися незалежності.

2.7.3 Необхідно ретельно обирати осіб, які отримуватимуть звіти про невідповідності або незаконні дії. Виникнення та вплив невідповідностей і незаконних дій є делікатним питанням, тому відправка звітів про них несе окремі ризики, включаючи:

- подальше зловживання вразливими місцями контролів внаслідок розкриття їх деталей;
- втрату клієнтів, постачальників та інвесторів у випадку санкціонованого або несанкціонованого розкриття інформації поза організацією;
- втрату ключових співробітників і керівників, у тому числі непричетних до невідповідностей і незаконних дій, внаслідок зниження впевненості в керівництві та майбутньому організації.

2.7.4 Фахівці повинні розглядати звітування про невідповідності та незаконні дії окремо від звітування про інші питання аудиту, якщо це сприятиме правильному розповсюдженню звітів.

2.7.5 Фахівці повинні намагатися уникати попередження осіб, пов'язаних з або причетних до невідповідностей і незаконних дій, з метою зменшення потенційного ризику знищення або приховання ними доказів.

2.7.6 Статут аудиту повинен встановлювати обов'язки фахівців щодо звітування про невідповідності та незаконні дії.

2207 Невідповідності та незаконні дії (продовження)

2.8 Зовнішнє звітування

2.8.1 Зовнішнє звітування про шахрайство, невідповідності та незаконні дії може бути правовим або регуляторним обов'язком. Такий обов'язок може покладатися на керівництво організації, осіб, відповідальних за виявлення невідповідностей, або обох з них. Законодавчі вимоги щодо звітування, які стоять перед аудитором, визначаються місцевою юрисдикцією і відміняють засади внутрішньої політики та / або договорів. Додаткові ситуації, за яких може виникнути необхідність зовнішнього звітування:
- дотримання правових або регуляторних вимог;
- судові рішення;
- фінансуючі організації або урядові органи у відповідності до вимог до аудиту суб'єктів, що отримують державну фінансову допомогу;
- запити зовнішніх аудиторів.

2.8.2 За умови зовнішнього звітування спершу відповідний рівень керівництва аудиту та підтвердження довіри до ІС повинен затвердити, а вище виконавче керівництво організації, що підлягає аудиту, перевірити форму та зміст інформації, наведеної у звітах, якщо це не суперечить діючим нормативним документам або особливим обставинам завдань з аудиту. Особливі обставини, за яких немає потреби в отриманні згоди вищого виконавчого керівництва організації, що підлягає аудиту:
- активна причетність вищого виконавчого керівництва організації, що підлягає аудиту, до невідповідностей і незаконних дій;
- пасивне допущення вищим виконавчим керівництвом організації, що підлягає аудиту, невідповідностей і незаконних дій.

2.8.3 Якщо вище виконавче керівництво організації, що підлягає аудиту, не дає згоду на зовнішнє розкриття відповідних звітів, а зовнішнє звітування є статутним або нормативним обов'язком, фахівці повинні проконсультуватися з аудиторським комітетом і юристом щодо доцільності та ризиків, пов'язаних зі звітуванням про такі результати поза межами організації. Навіть якщо фахівці захищені переважним правом, за таких обставин до розкриття звітів вони повинні звернутися за юридичною допомогою та консультацією, щоб переконатися у своїй захищеності таким переважним правом.

2.8.4 З дозволу керівництва аудиту та підтвердження довіри до ІС фахівці повинні своєчасно звітувати про невідповідності та незаконні дії відповідним регуляторним органам. Якщо організація відмовляється від розкриття виявлених невідповідностей і незаконних дій, або вимагає, щоб фахівці приховали їх, останні повинні звернутися за юридичною допомогою та консультацією.

2.8.5 У випадку виявлення фахівцями невідповідностей і незаконних дій, вони повинні своєчасно повідомити про них зовнішніх аудиторів.

2.8.6 Якщо фахівці знають, що керівництво зобов'язане звітувати про шахрайство зовнішнім організаціям, вони повинні офіційно повідомити керівництво про такий обов'язок.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами

3.2 Зв'язок із процесами COBIT 5

3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:
- найбільш придатні стандарти ISACA, які безпосередньо стосуються цієї настанови ;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1005 Належна професійна ретельність	Фахівці з аудиту та підтвердження довіри до ІС повинні проявляти належну професійну ретельність, у тому числі дотримуватись діючих професійних аудиторських стандартів при плануванні, виконанні та звітуванні за результатами завдань.

2207 Невідповідності та незаконні дії (продовження)

3.1 Зв'язок зі стандартами (продовження)

Назва стандарту	Відповідні положення стандарту
1201 Планування завдань	Фахівці з аудиту та підтвердження довіри до ІС повинні планувати кожне завдання з аудиту та підтвердження довіри до ІС таким чином, щоб воно відповідало: • цілі (цілям), обсягу, часовим рамкам і запланованим результатам; • діючим законам і професійним аудиторським стандартам; • застосуванню, за необхідності, ризик-орієнтованого підходу; • питанням, що виникають у зв'язку зі специфікою завдань; • вимогам до документації та звітності.
1202 Оцінювання ризиків при плануванні	Функція аудиту та підтвердження довіри до ІС повинна застосовувати необхідний підхід до оцінки ризиків та відповідну допоміжну методологію, щоб розробити загальний план аудиту ІС і визначити пріоритети для ефективного розподілу ресурсів аудиту ІС. При плануванні індивідуальних завдань фахівці з аудиту та підтвердження довіри до ІС повинні визначати та оцінювати ризики, пов'язані зі сферою, що перевіряється. Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики, пов'язані з об'єктом перевірки, аудиторські ризики та інші відповідні ризики для організації.
1207 Невідповідності та незаконні дії	При виконанні завдань фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики існування невідповідностей та незаконних дій. При виконанні завдань фахівці з аудиту та підтвердження довіри до ІС повинні дотримуватись позиції професійного скептицизму. Фахівці з аудиту та підтвердження довіри до ІС повинні документально оформляти та вчасно звітувати перед відповідними особами про будь-які значні невідповідності чи незаконні дії.
1401 Звітування	Фахівці з аудиту та підтвердження довіри до ІС повинні гарантувати, що наведені в аудиторському звіті результати ґрунтуються на достатніх та відповідних аудиторських доказах.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
• Процеси COBIT 5
• Цілі процесів COBIT 5
Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
EDM03 Забезпечувати оптимізацію ризиків	Забезпечити, щоб ризики організації, пов'язані з IT, не перевищували рівень її схильності та піддатливості ризикам, вплив ризиків, пов'язаних з IT, на вартість організації визначений і контролюється, а потенціал відхилень, пов'язаних з невідповідностями, мінімізований.
APO12 Управляти ризиками	Поєднати управління ризиками організації, пов'язаними з IT, із загальним управлінням ризиками організації та збалансувати витрати та переваги управління ризиками організації, пов'язаними з IT.
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.

2207 Невідповідності та незаконні дії (продовження)

3.2 Зв'язок із процесами COBIT 5 (продовження)

Процес COBIT 5	Мета процесу
MEA03 Відстежувати, оцінювати та аналізувати відповідність зовнішнім вимогам	Забезпечити дотримання організацією діючих зовнішніх вимог.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
- у колег, що працюють в організації;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- у професійних організаціях;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Невідповідність	Порушення встановленої політики управління чи регуляторної вимоги. Наприклад, навмисна подача недостовірної інформації або упущення інформації стосовно сфери, яка підлягає аудиту, або організації в цілому, що свідчить про грубу недбалість або ненавмисне вчинення незаконних дій.
Професійний скептицизм	Ставлення, яке включає допитливе мислення та критичну оцінку аудиторських доказів. Джерело: AU 230.07, AICPA.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2208 Вибірка

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови полягає у наданні фахівцям з аудиту та підтвердження довіри до ІС вказівок щодо планування та здійснення аудиторської вибірки та оцінювання її результатів. Належна вибірка та оцінювання сприятимуть виконанню вимог щодо достатності та відповідності доказів.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1006 Професійність
1.2.2 Стандарт 1202 Оцінювання ризиків при плануванні
1.2.3 Стандарт 1203 Ефективність і нагляд
1.2.4 Стандарт 1205 Докази

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані зі завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Вибірка
2.2 Планування вибірки
2.3 Здійснення вибірки
2.4 Оцінювання результатів вибірки
2.5 Документальне оформлення

2.1 Вибірка

2.1.1 При формуванні професійної думки чи висновків фахівці, як правило, перевіряють не всю доступну інформацію, оскільки це непрактично (наприклад, як організації, що підлягає аудиту, так і фахівцям необхідно занадто багато часу для дослідження всієї інформації), а обґрунтовані висновки можна отримати за допомогою аудиторської вибірки.

2.1.2 Застосовуючи статистичні або нестатистичні методи вибірки, фахівці повинні планувати і здійснювати аудиторську вибірку, виконувати аудиторські процедури та оцінювати результати вибірки з метою отримання достатніх і відповідних доказів для формування висновків. Застосовуючи методи вибірки для формування висновків щодо всієї сукупності значень, фахівці повинні використовувати статистичну вибірку.

2.2 Планування вибірки

2.2.1 Плануючи розмір і структуру аудиторської вибірки, фахівці повинні враховувати конкретні цілі аудиту ІС, аудиторські процедури, за допомогою яких можна досягти такі цілі, характер сукупності значень, відповідні підгрупи такої сукупності значень, а також методи вибірки та її здійснення. Окрім того, за умови відповідності аудиторської вибірки необхідно розглянути характер отриманих доказів, а також можливі умови виникнення помилок і їхні першопричини.

2.2.2 При плануванні аудиторської вибірки, окрім цілей аудиту ІС, фахівці повинні враховувати:
- призначення вибірки;
- елементи вибірки;

2208 Вибірка (продовження)

2.2 Планування вибірки (продовження)

- сукупність значень;
- ризики вибірки та її розмір;
- припустимі помилки;
- базовий очікуваний розподіл (наприклад, пуассонівський, біноміальний, нормальний або експоненційний);
- поведінку в довготривалій перспективі (наприклад, сезонний фактор або спад діяльності);
- підсукупності або підгрупи значень, які є природними і повинні враховуватися для визначення відповідності функціонування;
- викиди;
- малі сукупності значень небажаних або рідкісних явищ;
- дані інструментів зовнішньої підтримки, що застосовуються для підтвердження або доповнення результатів вибірки.

2.2.3 Фахівці повинні враховувати мету формування вибірки:

- **перевірка на відповідність / перевірка контролів** (аудиторська процедура, розроблена для оцінювання ефективності функціонування контролів з метою попередження або виявлення та виправлення значних вразливих місць; прикладами перевірки контролів на відповідність, коли можна розглядати застосування вибірки, є права доступу користувачів, процедури контролю зміни програм, процедури документального оформлення, програмна документація, подальший контроль порушень, перевірка контрольних журналів та аудит ліцензій на програмне забезпечення);
- **перевірка на суттєвість / перевірка деталей** (аудиторська процедура, розроблена для вижявлення значних вразливих місць на рівні тверджень; прикладами перевірки на суттєвість, коли можна розглядати застосування вибірки, є повторне проведення комплексних розрахунків (наприклад, відсотків) при вибірці рахунків, вибірка транзакцій при перевірці супровідної документації тощо).

2.2.4 Елементи вибірки залежать від її призначення. При перевірці контролів на відповідність, коли елементами вибірки є події або транзакції (наприклад, такі контролі, як авторизація рахунків-фактур), атрибутивна вибірка, як правило, застосовується для визначення характеристик сукупності значень. При перевірці на суттєвість, коли елементи вибірки часто є грошовими, як правило, застосовується кількісна вибірка, оскільки її ціллю є визначення грошового або волюметричного обсягу характеристик сукупності значень.

2.2.5 Сукупність значень є всією множиною даних, з якої фахівці роблять вибірку для формування висновків щодо сукупності значень. Таким чином, сукупність значень, з якої робиться вибірка, повинна бути відповідною для перевірки ефективності розробки та / або функціонування контролів і повною в рамках конкретних цілей та обсягу аудиту ІС.

2.2.6 Для ефективного та дієвого планування вибірки може знадобитися стратифікація вибірки. Стратифікація – це процес поділу сукупності значень на підсукупності значень зі схожими та чітко визначеними характеристиками, щоб кожний елемент вибірки належав лише до одного стратуму.

2.2.7 При визначенні розміру вибірки фахівці повинні враховувати ризики вибірки, прийнятну кількість помилок та їх очікуваний обсяг. Ризики вибірки виникають внаслідок існування ймовірності того, що висновки фахівців можуть різнитися від висновків, яких можна було б досягти при здійсненні аналогічних аудиторських процедур над усією сукупністю. Існує два типи ризиків вибірки:

- **ризики помилкового прийняття** (значний недолік оцінюється як маловірогідний у той час, як сукупність значень є фактично неправильно сформульованою);
- **ризики помилкового неприйняття** (значний недолік оцінюється як вірогідний у той час, як сукупність значень є фактично правильно сформульованою).

2.2.8 На розмір вибірки впливає рівень її ризиків, який має бути прийнятним для фахівців. Окрім того, ризики вибірки необхідно розглядати стосовно моделі ризиків аудиту та її складових, ризиків, притаманних організації, ризиків системи контролів і ризиків невиявлення помилок, що детально описано у Стандарті 2202 «Оцінювання ризиків при плануванні».

2.2.9 Припустимі помилки – це максимальні помилки сукупності значень, які є прийнятними для фахівців і дозволяють досягти цілей перевірки. У випадку перевірки на суттєвість припустимі помилки пов'язані з судженням фахівців щодо суттєвості. У випадку перевірки на відповідність вони є максимальним рівнем відхилень від встановлених процедур контролів, які є прийнятним для фахівців.

2208 Вибірка (продовження)

2.2 Планування вибірки (продовження)

2.2.10 Якщо фахівці вважають ймовірною наявність помилок у сукупності значень, необхідно оцінювати більшу вибірку, ніж у випадку відсутності помилок, щоб дійти висновків щодо того, що фактичні помилки у сукупності значень не перевищують очікуваного рівня припустимих помилок. Менші розміри вибірки оправдані, коли у сукупності значень не припускають наявності помилок. При оцінюванні очікуваних помилок у сукупності значень фахівці повинні враховувати наступне:
- рівень виявлених помилок у минулих аудитах;
- зміни в процедурах організації;
- докази, отримані при оцінюванні системи внутрішніх контролів, результати процедур аналітичних перевірок та / або результати попередніх перевірок сукупності значень.

2.2.11 За необхідності, фахівці повинні розглядати потребу залучення фахівців до розробки та аналізу комплексних підходів до вибірки, наприклад, стратифікованої випадкової вибірки, яка повинна бути статистично обґрунтованою, або вибірки за допомогою встановлених методів контролю довіри до (наприклад, «Шість сигма»).

2.2.12 Якщо фахівці приходять до висновків, що вибірка не дозволяє досягти цілі аудиту ІС, і необхідна перевірка всієї сукупності значень, вони повинні розглядати застосування тривалого підтвердження довіри, яке забезпечує своєчасну та економічно вигідну перевірку всієї сукупності значень. Детальні вказівки щодо цього питання наведено у Настанові 2211 «Тривале підтвердження довіри».

2.3 Здійснення вибірки

2.3.1 Фахівці повинні забезпечити повноту сукупності значень і контролювати здійснення вибірки з метою дотримання аудиторської незалежності. Фахівці повинні здійснювати вибірку таким чином, щоб вона представляла всю сукупність значень, враховуючи характеристики, що перевіряються.

2.3.2 Оскільки вибірка представляє всю сукупність значень, кожний елемент вибірки із цієї сукупності повинна мати однакову або відому ненульову ймовірність потрапляння у вибірку. Це означає необхідність застосування статистичних методів вибірки, оскільки вони використовують такі методики, за допомогою яких математичним способом можна досягти висновків щодо всієї сукупності значень. Таким чином, фахівці повинні підтверджувати повноту сукупності значень для забезпечення здійснення вибірки з належної множини даних.

2.3.3 Нестатистична вибірка є підходом фахівців, які для визначення вибірки застосовують власний досвід, знання і професійні судження. Такий метод припускає наявність суб'єктивних систематичних похибок, оскільки він не ґрунтується на статистичних даних і не забезпечує те, що кожний елемент вибірки має однакову або відому ненульову ймовірність потрапляння у вибірку. Таким чином, результати такого методу не повинні поширюватися на всю сукупність значень, оскільки маловірогідне, що вибірка представляє всю сукупність значень. Нестатистичну вибірку можна застосовувати за необхідності швидкого підтвердження питання і не слід застосовувати для досягнення висновків щодо всієї сукупності значень математичним способом.

2.3.4 Існує п'ять загальноприйнятих методів вибірки, які поділяють на статистичні або нестатистичні.
- Статистичні методи вибірки:
  - **проста випадкова вибірка** (забезпечує однакову ймовірність потрапляння у вибірку всіх поєднань її елементів у сукупності значень);
  - **систематична вибірка** (забезпечує вибірку елементів за умови фіксованих інтервалів між здійсненням вибору з випадковим початком першого інтервалу; наприклад, монетарна вибірка або вибірка виміру вартості, за якої кожна окрема грошова величина (наприклад, $ 1 000) у сукупності значень має однакову ймовірність потрапляння у вибірку; враховуючи те, що, як правило, не можна окремо розглядати монетарні одиниці, у вибірку потрапляє елемент, який містить їх; такий метод систематично впливає на здійснення вибірки на користь більших величин; іншим прикладом є вибір кожного енного елементу);
  - **стратифікована випадкова вибірка** (забезпечує те, що кожний елемент вибірки з кожної підгрупи має відому ненульову ймовірність потрапляння у вибірку).

Фахівці повинні розглядати застосування статистичного програмного забезпечення для підрахування стандартних відхилень та інших сумарних статистик для отримання результатів статистичної вибірки.
- Нестатистичні методи вибірки:
  - **безсистемна вибірка** (фахівці здійснюють вибірку, не застосовуючи жодних структурованих методик та уникаючи будь-яких свідомих упереджень або передбачуваності; однак, на аналіз

2208 Вибірка (продовження)

2.3 Здійснення вибірки (продовження)

такої вибірки не слід надіятися при формуванні висновків щодо сукупності значень);
– **детермінована вибірка** (фахівці враховують похибку вибірки (наприклад, усі елементи вибірки з певної величини, усі елементи вибірки з певного типу винятків або усі елементи вибірки з від'ємних); необхідно враховувати, що така вибірка не є статистично обґрунтованою, а також що її результати не повинні поширюватися на всю сукупність значень, оскільки маловірогідно, що вибірка представляє сукупність значень в цілому).

2.3.5 Існує два загальноприйнятих методу здійснення вибірки:
- вибірка із записів і сукупності значень підгруп за допомогою наступних методів:
  – простої випадкової вибірки;
  – стратифікованої випадкової вибірки;
  – безсистемної вибірки;
  – детермінованої вибірки;
- вибірка із кількісних сфер (наприклад, грошових одиниць) за допомогою наступних методів:
  – простої випадкової вибірки;
  – систематичної вибірки.

2.4 Оцінювання результатів вибірки

2.4.1 Після виконання аудиторських процедур, відповідних для досягнення цілей аудиту ІС, для кожного елемента вибірки фахівці повинні проаналізувати всі можливі помилки, виявлені у вибірці, для визначення того, чи вони дійсно є помилками, а також, за необхідності, їх характеру та причин виникнення. Ті помилки, які оцінюються як актуальні, за необхідності, потрібно спроектувати на сукупність значень, але лише за умови застосування статистичних методів вибірки.

2.4.2 Усі можливі помилки, виявлені у вибірці, необхідно перевірити з метою визначення того, чи вони дійсно є помилками. Фахівці повинні враховувати якісні аспекти помилок, включаючи характер і причини виникнення помилок, а також їх можливий вплив на інші фази аудиту. Наприклад, помилки, які виникають внаслідок збоїв автоматизованих процесів, як правило, мають ширші наслідки, ніж викликані людським фактором.

2.4.3 У випадку неможливості отримання очікуваних аудиторських доказів стосовно певного елемента вибірки фахівці повинні розглядати можливість отримання ними достатніх і відповідних аудиторських доказів за допомогою альтернативних процедур над обраним елементом вибірки або вибір і перевірку іншого елементу.

2.4.4 Фахівці повинні враховувати планування результатів вибірки на загальну сукупність значень за допомогою методу планування разом із методом формування пробної вибірки. Планування вибірки може включати в себе оцінювання можливих помилок у сукупності значень, а також усіх подальших помилок, які могли бути невиявленими внаслідок неточності методики, враховуючи якісні аспекти всіх виявлених помилок.

2.4.5 Обговорення результатів нестатистичної вибірки (безсистемної або детермінованої) повинно обмежуватись описом результатів аналізу вибірки в контексті сукупності значень в цілому.

2.4.6 Фахівці повинні враховувати, чи помилки у сукупності значень можуть перевищувати припустимі помилки, шляхом порівняння спроектованих на сукупність значень помилок з оціненими або визначеними припустимими помилками, враховуючи результати інших аудиторських процедур, пов'язаних із цілями аудиту. Припустимі помилки можуть оцінюватися або визначатися за допомогою критеріїв аудиту, галузевих стандартів, контрактних вимог, специфікацій програмного забезпечення тощо. Якщо помилки у сукупності значень перевищують припустимі помилки, фахівці повинні здійснити повторне оцінювання ризиків вибірки, а також у випадку неприйнятності таких ризиків розглянути розширення процедур аудиту, перерахування розміру вибірки за допомогою оброблених припустимих помилок, перевірку додаткових елементів вибірки або здійснення альтернативних процедур аудиту.

2.5 Документальне оформлення

2.5.1 Для чіткого опису цілей і процесу вибірки робоча документація повинна містити достатню кількість інформації, у тому числі:
- призначення вибірки, включаючи елементи вибірки;
- джерела та визначення сукупності значень, а також її зв'язок із обсягом аудиту;
- параметри вибірки, наприклад, її розмір (враховуючи ризики вибірки), випадковий початок, початковий номер або метод визначення випадкового початку, інтервалу вибірки;
- методи формування вибірки;
- обрані елементи, а також обґрунтування їх вибору у випадку нестатистичної вибірки;

2208 Вибірка (продовження)

2.5 Документальне оформлення (продовження)

- деталі виконаних аудиторських перевірок, включаючи оцінювання помилок і, за необхідності, альтернативні процедури аудиту;
- отримані висновки.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами
3.2 Зв'язок із процесами COBIT 5
3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA щодо аудиту та підтвердження довіри до ІС, які безпосередньо стосуються цієї настанови ;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1006 Професійність	Фахівці з аудиту та підтвердження довіри до ІС, а також інші особи, які допомагають у виконанні поставлених завдань, повинні колективно володіти необхідними навичками і проявляти професійність при виконанні завдань з аудиту та підтвердження довіри до ІС, а також бути професійно компетентними для здійснення роботи.
1202 Оцінювання ризиків при плануванні	Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати ризики, пов'язані з об'єктом перевірки, ризики аудиту та інші відповідні ризики для організації.
1203 Ефективність і нагляд	Для досягнення цілей аудиту фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази. Аудиторські результати та висновки повинні супроводжуватись відповідним аналізом та тлумаченням таких доказів. Фахівці з аудиту та підтвердження довіри до ІС повинні документально оформляти процес аудиту, описуючи аудиторську роботу та аудиторські докази, що обґрунтовують результати та висновки. Фахівці з аудиту та підтвердження довіри до ІС повинні визначати та робити висновки щодо результатів.
1205 Докази	Фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази, щоб зробити обґрунтовані висновки, на які спиратимуться результати завдань. Фахівці з аудиту та підтвердження довіри до ІС повинні оцінювати достатність отриманих доказів для обґрунтування висновків та досягнення цілей завдань.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:

- Процеси COBIT 5
- Цілі процесів COBIT 5

Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
APO12 Управляти ризиками	Поєднати управління ризиками організації, пов'язаними з IT, із загальним управлінням ризиками організації та збалансувати витрати та переваги управління ризиками організації, пов'язаними з IT.

2208 Вибірка (продовження)

3.2 Зв'язок із процесами COBIT 5 (продовження)

Процес COBIT 5	Мета процесу
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.
MEA03 Відстежувати, оцінювати та аналізувати відповідність зовнішнім вимогам	Забезпечити дотримання організацією діючих зовнішніх вимог.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
- у колег, що працюють в організації;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- у професійних організаціях;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Атрибутивна вибірка	Метод вибору частини з сукупності значень, ґрунтуючись на наявності або відсутності певних характеристик.
Аудиторська вибірка	Застосування аудиторських процедур до менше ніж 100 відсотків елементів в сукупності значень для отримання аудиторських доказів щодо певних характеристик сукупності значень
Вибірка змінного обсягу	Методика формування вибірки, яка застосовується для оцінювання середньої або загальної величини в сукупності значень, ґрунтуючись на вибірці. Статистична модель, яка застосовується для прогнозування кількісних характеристик, наприклад, грошових сум.
Нестатистична вибірка	Метод вибору частини з сукупності значень шляхом застосування професійних суджень і власного досвіду з метою швидкого підтвердження судження. Такий метод не надає можливості застосовувати математичні висновки для всієї сукупності значень.
Припустима похибка	Максимальна похибка сукупності значень, яка є прийнятною для фахівців і дозволяє досягти цілі перевірки. У випадку перевірки на суттєвість припустимі помилки пов'язані із судженнями фахівців щодо суттєвості. У випадку перевірки на відповідність вони є максимальним рівнем відхилень від встановлених процедур контролів, які є прийнятним для фахівців.
Ризик вибірки	Ймовірність того, що аудитори ІС дійшли неправильних висновків внаслідок перевірки аудиторської вибірки, а не всієї сукупності значень. **Обмежуюча примітка.** Ризик вибірки неможливо виключити, їх можна лише зменшити до прийнятно низького рівня, розглядаючи відповідні обсяг вибірки та метод її формування.
Статистична вибірка	Метод вибору частини з сукупності значень шляхом здійснення математичних розрахунків і визначення ймовірностей з метою досягнення науково і математично обґрунтованих висновків щодо характеристик усієї сукупності значень.
Стратифікація вибірки	Процес поділу сукупності значень на підсукупності значень зі схожими чітко визначеними характеристиками таким чином, щоб кожний елемент вибірки належав лише до одного стратуму.

2208 Вибірка (продовження)

4. Термінологія (продовження)

Термін	Визначення
Сукупність значень	Уся множина даних, з якої робиться вибірка, стосовно якої аудитори ІС мають наміри дійти до висновків.

5. Дата набуття чинності та дата перегляду

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

Настанови щодо звітування

Настанови щодо звітування:
2401 Звітування
2402 Подальша діяльність

Усі настанови описані тут вичерпно. Посилання на окремі стандарти можна отримати на наступній сторінці: www.isaca.org/standard.

2401 Звітування

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Ця настанова надає фахівцям з аудиту та підтвердження довіри до ІС вказівки щодо різних типів завдань з аудиту ІС і пов'язаних з ними звітів.

1.1.2 Ця настанова детально описує всі аспекти, які необхідно включати у звіти про завдання з аудиту, і надає фахівцям з аудиту та підтвердження довіри до ІС фактори, які необхідно враховувати при підготовці проектів і завершенні формування звітів про аудиторські завдання.

1.1.3 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1007 Твердження
1.2.2 Стандарт 1205 Докази
1.2.3 Стандарт 1401 Звітування
1.2.4 Стандарт 1402 Подальша діяльність

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані зі завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Типи завдань
2.2 Необхідний зміст звітів про завдання з аудиту
2.3 Подальші події
2.4 Додаткове звітування

2.1 Типи завдань

2.1.1 Фахівці можуть виконувати будь-які з наступних типів завдань з аудиту:
- перевірку;
- перегляд;
- узгоджені процедури.

Примітка. Ці терміни визначені в «ITAF. 2-ге видання».

2.1.2 Завдання як з перевірки, так і з перегляду передбачають:
- планування завдань;
- оцінювання ефективності розробки процедур контролів;
- перевірка ефективності функціонування процедур контролів (характер, часові рамки та обсяг перевірки можуть різнитися залежно від типу завдань);
- формування висновків і звітування про ефективність розробки та / або функціонування процедур перевірки контролю, ґрунтуючись на виявлених критеріях:
  – висновки з надання достатньої впевненості у завданнях є позитивними і забезпечують високий рівень впевненості;
  – висновки з надання обмеженої впевненості у завданнях є негативними і забезпечують лише помірний рівень впевненості.

2.1.3 Здійснюючи «узгоджені процедури» завдань фахівці не надають жодних гарантій. Фахівці

2401 Звітування (продовження)

2.1 Типи завдань (продовження)

залучаються до виконання певних процедур з метою задоволення інформаційних потреб осіб, які узгодили виконання таких процедур (наприклад, вищого виконавчого керівництва, ради або осіб, відповідальних за корпоративне управління). Фахівці надають звіти про фактологічні результати особам, які узгодили виконання таких процедур. Одержувачі формують свої власні висновки, ґрунтуючись на таких звітах, оскільки характер, часові рамки та обсяг процедур не дозволяють надання впевненості фахівцями. Такі звіти відправляються лише особам, які узгодили виконання таких процедур, оскільки інші особи не знають причин таких процедур і можуть неправильно зрозуміти їх результати.

2.1.4 Звіти про узгоджені процедури також можна розкривати третім особам (наприклад, регуляторним органам) за умови попереднього встановлення і затвердження особами, які узгодили виконання таких процедур, до початку фактичної роботи. Фахівці повинні розглядати це, застосовуючи свої професійні судження і враховуючи ризик неправильного тлумачення роботи, що підлягає виконанню.

2.1.5 Фахівці, які до завершення завдань з аудиту отримують вимогу про зміну типу таких завдань з перевірки чи перегляду на виконання узгоджених процедур, повинні враховувати доречність такої зміни і не повинні погоджуватися на неї без видимих причин. Наприклад, зміна є недоречною, якщо вона націлена на ухилення від кваліфікованого висновку.

2.2 Необхідний зміст звітів про завдання з аудиту

2.2.1 При підготовці звітів про завдання з аудиту необхідно враховувати всі отримані відповідні докази, незалежно від підтвердження чи заперечення ними інформації щодо об’єкта перевірки. Якщо існують професійні судження , їх повинні обґрунтовувати результати процедур перевірки контролю за допомогою виявлених критеріїв. Фахівці повинні отримати достатні та відповідні докази для обґрунтування своїх висновків у звітах про завдання з аудиту. Детальніші вказівки наведено у Стандарті 1205 «Докази».

2.2.2 При формуванні висновків про завдання з перевірки чи перегляду фахівці повинні висловлювати свої професійні судження про ефективність розробки та / або функціонування процедур контролів сфери діяльності в усіх важливих відношеннях, а саме:

- **некваліфіковані професійні судження** (якщо фахівці доходять висновку про ефективність розробки та / або функціонування процедур контролів сфери діяльності згідно з відповідними критеріями в усіх важливих відношеннях);
- **кваліфіковані професійні судження** (якщо фахівці:
  - отримують достатні та відповідні докази і доходять висновку про те, що вразливі місця контролів індивідуально або у сукупності є значними, але не поширюються на цілі аудиту ІС;
  - не можуть отримати достатніх та відповідних доказів для обґрунтування своїх професійних міркувань , але доходять висновку про те, що можливий вплив невиявлених вразливих місць контролів, якщо такі існують, може бути значним, але не поширюватиметься на цілі аудиту ІС);
- **несприятливі професійні судження** (якщо одне чи кілька значних порушень у сукупності призводять до значних і широко розповсюджених вразливих місць);
- **відмову** (фахівці відмовляються від надання своїх професійних суджень, якщо вони не можуть отримати достатніх і відповідних доказів для їхнього обґрунтування та доходять висновку про те, що можливий вплив невиявлених вразливих місць контролів, якщо такі існують, може бути значним і поширюватиметься на цілі аудиту ІС).

2.2.3 Звіт фахівців про перевірку чи перегляд ефективності процедур контролів повинен містити наступні елементи:

- відповідну та виразну назву, завдяки якій звіт відрізнятиметься від звітів інших типів, на які не поширюються стандарти аудиту;
- одержувачів звіту згідно з умовами статуту аудиту або контракту;
- відповідальних осіб, у тому числі положення осіб, відповідальних за об’єкт перевірки;
- опис обсягу завдань з аудиту, назви установи або частини установи, пов’язаної з об’єктом перевірки, включаючи:

2401 Звітування (продовження)

2.2 Необхідний зміст звітів про завдання з аудиту (продовження)

– визначення або опис сфери діяльності;
– критерії, на яких ґрунтуються висновки фахівців;
– момент або період часу, пов'язаний з роботою над об'єктом перевірки, його оцінюванням або вимірюванням;
– положення про відповідальність керівництва за забезпечення ефективної структури внутрішніх контролів, у тому числі процедур контролів сфери діяльності;

- положення, що визначає джерела звернень керівництва щодо ефективності процедур контролів;
- положення щодо проведення фахівцями завдань з аудиту та висловлення власних професійних суджень про ефективність процедур контролів;
- визначення мети (тобто цілей аудиту ІС), в рамках якого сформовано звіти фахівців, осіб, які можуть покладатися на них, і відмову від відповідальності за їх застосування не за призначенням або іншими особами;
- опис критеріїв або розкриття їх джерел; більше того, фахівці повинні розглядати розкриття:
  – усіх значущих тлумачень, отриманих при застосуванні критеріїв;
  – методів вимірювання, що застосовуються, якщо критерії надають декілька таких методів на вибір;
  – змін стандартних методів вимірювання, що застосовуються;
- положення щодо проведення завдань з аудиту у відповідності до стандартів аудиту та підтвердження довіри до ІС ISACA або інших відповідних професійних стандартів; недотримання таких стандартів необхідно чітко зазначати у звіті;
- подальші пояснення щодо змінних, які впливають на підтвердження довіри до ІС, а також, за необхідності, на іншу інформацію;
- результати, висновки і рекомендації щодо корегуючих заходів і відгуки керівництва; при отриманні кожного відгуку керівництва фахівці повинні отримувати інформацію щодо виконання запропонованих заходів або розгляду рекомендацій, про які йдеться у звіті, а також щодо запланованого терміну такого виконання або розгляду:
  – відповідальне керівництво може вирішити прийняти ризик невиправлення обставин, про які йдеться у звіті, у зв'язку з вартістю, складністю корегуючих заходів або іншими факторами, які необхідно враховувати; необхідно інформувати раду директорів (або осіб, відповідальних за корпоративне управління) про рекомендації, щодо яких керівництво приймає ризик невиправлення ситуації, про яку йдеться у звіті;
  – якщо фахівці та організація, що підлягає аудиту, не погоджуються з певними рекомендаціями або аудиторськими коментарями, в аудиторській звітності можуть вказуватися як позиції, так і причини такої незгоди; письмові коментарі організації, що підлягає аудиту, можуть бути додатком до звіту про завдання; і навпаки, точка зору організації, що підлягає аудиту, може міститися в основній частині звіту або у супровідному листі; вище виконавче керівництво або особи, відповідальні за корпоративне управління, повинні приймати рішення, чию точку зору вони підтримують;
- параграф, у якому йдеться про те, що у зв'язку із системними обмеженнями будь-яких внутрішніх контролів можуть виникати і залишатися невиявленими недостовірності, спричинені помилками або шахрайством; окрім того, у такому параграфі повинно йтися про те, що проектування будь-яких оцінок внутрішніх контролів з фінансових звітів на майбутні періоди створюють ризик невідповідності внутрішніх контролів внаслідок зміни обставин або зменшення рівня відповідності політикам і процедурам; мета розробки завдань з аудиту не полягає у виявленні всіх вразливих місць процедур контролів, оскільки вони не виконуються безперервно протягом усього періоду, окрім того, перевірки процедур контролів здійснюються вибірково;
- стислий опис виконаної роботи, який сприятиме кращому розумінню цільовими користувачами звіту характеру підтвердження довіри, яке проводиться;
- висловлення професійних суджень щодо ефективності розробки та / або функціонування процедур контролів сфери діяльності в усіх важливих відношеннях; якщо професійні судження фахівців є кваліфікованими, параграф, що описує причини кваліфікації;
- за необхідності, посилання на усі інші звіти, які слід враховувати, наприклад, на окремі звіти про вразливості системи безпеки, захищені від розкриття, повинні відправлятися обмеженому списку одержувачів;

2401 Звітування (продовження)

2.2 Необхідний зміст звітів про завдання з аудиту (продовження)

- дата опублікування звіту про завдання з аудиту; у більшості випадків дата звіту ґрунтується на даті його опублікування; також рекомендується зазначати такі дати при фактичному завершенні виконання аудиторської роботи, якщо вони не зазначалися у стислому викладі виконаної роботи;
- імена осіб і назви установ, відповідальних за звіти, відповідні підписи та місцезнаходження.

2.2.4 Звіт про узгоджені процедури повинен подаватися у формі процедур і результатів і містити наступні елементи:

- відповідну та виразну назву, завдяки якій звіт відрізнятиметься від звітів інших типів, на які не поширюються стандарти аудиту;
- одержувачів, яким направлятиметься звіт згідно з умовами статуту аудиту;
- відповідальних осіб, у тому числі положення осіб, відповідальних за об'єкт перевірки;
- положення щодо проведення завдань з аудиту у відповідності до стандартів аудиту та підтвердження довіри до ІС ISACA або інших відповідних професійних стандартів; недотримання таких стандартів необхідно чітко зазначати у звіті;
- визначення об'єкта перевірки (або пов'язаного з ним письмового твердження) та мети завдань з аудиту (тобто цілей аудиту ІС);
- положення про затвердження відповідних процедур відповідальними сторонами, вказаними у звіті;
- положення про повну та одноосібну відповідальність замовників за достатність процедур і про відмову від відповідальності виконавців за достатність таких процедур;
- список здійснених процедур (або посилання на нього);
- опис результатів, включаючи достатню деталізацію виявлених помилок і порушень;
- положення про те, що фахівці виконали узгоджені процедури без здійснення підтвердження довіри як такого;
- положення про те, що при виконанні додаткових процедур фахівці могли звернути увагу на інші питання і зазначити їх у звіті;
- положення про обмеження, пов'язані з використанням звіту, внаслідок його призначення виключно визначеними сторонами;
- положення про те, що звіт охоплює лише зазначені елементи і не поширюється за їх межі;
- посилання на усі інші звіти, які слід враховувати;
- дата опублікування звіту про завдання з аудиту; у більшості випадків дата звіту ґрунтується на даті його опублікування; також рекомендується зазначати такі дати при фактичному завершенні виконання аудиторської роботи, якщо вони не зазначалися у стислому викладі виконаної роботи;
- імена осіб і назви установ, відповідальних за звіти, відповідні підписи та місцезнаходження.

2.2.5 Існує два типи звітів про перевірку:

- **прямі звіти** (про об'єкт перевірки, а не про твердження; такий звіт повинен посилатися лише на об'єкт перевірки завдань і не повинен містити жодних посилань на твердження керівництва про об'єкт перевірки);
- **непрямі звіти** (ґрунтується на твердженнях керівництва про об'єкт перевірки).

Детальніші вказівки щодо різниці між непрямим і прямим звітуванням наведено у Стандарті 1007 «Твердження».

2.3 Подальші дії

2.3.1 Інколи певні дії можуть відбуватися після моменту або періоду перевірки об'єкта перевірки, але до дати звіту фахівців, що значним чином впливає на об'єкт перевірки і, відповідно, вимагає зміни або розкриття даних про об'єкт перевірки або твердження. Такі події іменуватимуться як подальші дії. При виконанні завдань з аудиту фахівці повинні розглядати інформацію про подальші дії, на які вони звертають увагу. Однак, фахівці не несуть відповідальність за виявлення подальших дій.

2.3.2 Фахівці повинні переконатися, чи знає керівництво про подальші дії (до дати звіту фахівців), які можуть значним чином впливати на об'єкт перевірки або твердження.

2.4 Додаткове звітування

2.4.1 Фахівці повинні обговорювати з керівництвом зміст проектів звітів у предметній сфері до підготовки та публікування заключного звіту і, за необхідності, включати в заключний звіт відгуки керівництва щодо результатів, висновків і рекомендацій.

2.4.2 Фахівці повинні звітувати про суттєві недоліки та значні порушення контрольного середовища особам, відповідальним за корпоративне управління, і, за необхідності, відповідальним

2401 Звітування (продовження)

2.4 Додаткове звітування (продовження)

повноважним особам. Окрім того, вони повинні чітко розкривати у своїх звітах факт такого звітування.

2.4.3 Фахівці повинні звітувати керівництву про внутрішні проблеми порушення контролів, які є меншими, ніж значні, але більшими, ніж незначні. У таких випадках фахівці повинні повідомляти осіб, відповідальних за корпоративне управління, або відповідальних повноважних осіб про інформування керівництва про такі внутрішні проблеми порушення контролів.

2.4.4 Фахівці повинні отримувати письмові звернення керівництва, які підтверджують щонайменше наступні твердження:

- керівництво несе відповідальність за встановлення і дотримання належних ефективних внутрішніх контролів, у тому числі контролів систем внутрішньої бухгалтерської звітності та адміністративних контролів операційної діяльності та інформаційних систем, що переглядаються, а також за діяльність, пов'язану з визначенням і дотриманням законів, правил і нормативних документів, які регулюють предметну сферу, що переглядається;
- групі, що займається завданнями, надається уся необхідна інформація, пов'язана із такими завданнями, включаючи, але не обмежуючись:
  – записами, пов'язаними даними, електронними файлами та звітами;
  – політиками і процедурами;
  – правильно підібраним персоналом;
  – результатами відповідних внутрішніх і зовнішніх аудитів ІС, переглядів та оцінювань;
- після завершення збору даних не відбулася жодна подія та не було виявлене жодне питання, які можуть значним чином впливати на завдання;
- керівництву не відомо про жодне реальне або припустиме шахрайство, невідповідність або незаконну дію, пов'язану з предметною сферою, що переглядається, включаючи нерозкрите керівництво та співробітників, обов'язком яких є забезпечення внутрішніх контролів;
- керівництву не відомо про жодну заяву про реальне або припустиме шахрайство, невідповідність або незаконну дію, яка впливає на предметну сферу, що переглядається, отриману від нерозкритих співробітників, клієнтів, підрядників або інших осіб;
- прийняття відповідальності за розробку і впровадження програм і контролів для запобігання і виявлення шахрайства, невідповідностей і незаконних дій.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами
3.2 Зв'язок із процесами COBIT 5
3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні і стандарти ISACA щодо аудиту та підтвердження довіри до ІС, які безпосередньо стосуються цієї настанови ;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1007 Твердження	Фахівці з аудиту та підтвердження довіри до ІС повинні перевіряти твердження, на основі яких здійснюватиметься оцінювання об'єкта перевірки, для визначення того, чи такі твердження можна піддати аудиту, і чи є вони достатніми, обґрунтованими та відповідними.
1205 Докази	Фахівці з аудиту та підтвердження довіри до ІС повинні отримати достатні та відповідні докази, щоб зробити обґрунтовані висновки, на які спиратимуться результати завдань. Фахівці з аудиту та підтвердження довіри до ІС повинні оцінювати достатність отриманих доказів для обґрунтування висновків та досягнення цілей завдань.

2401 Звітування (продовження)

3.1 Зв'язок зі стандартами (продовження)

Назва стандарту	Відповідні положення стандарту
1401 Звітування	Фахівці з аудиту та підтвердження довіри до ІС повинні звітувати про результати виконаних завдань, включаючи: • ідентифікацію організації, припустимого одержувача та будь-які обмеження щодо змісту та розповсюдження; • обсяг, цілі та період виконання завдань, а також характер, визначення терміну проведення та обсягу роботи, що підлягає здійсненню; • результати, висновки та рекомендації; • будь-які кваліфікації фахівців з аудиту та підтвердження довіри до ІС чи обмеження обсягу робіт, що стосуються виконання завдань; • підпис, дату та розповсюдження згідно з умовами статуту аудиту та контракту. Фахівці з аудиту та підтвердження довіри до ІС повинні гарантувати, що наведені в аудиторському звіті результати ґрунтуються на достатніх та відповідних аудиторських доказах.
1402 Подальша діяльність	Фахівці з аудиту та підтвердження довіри до ІС повинні виконувати відстеження відповідної інформації, щоб зробити висновок, чи керівництво своєчасно запланувало / вжило необхідні заходи для розгляду результатів та рекомендацій аудиторського звіту.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:
• Процеси COBIT 5
• Цілі процесів COBIT 5
Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

Процес COBIT 5	Мета процесу
EDM05 Забезпечувати прозорість для зацікавлених сторін	Забезпечити ефективність і своєчасність звітування зацікавленим сторонам, а також встановити підґрунтя звітування для підвищення ефективності, визначення сфер для такого покращення та підтвердження відповідності цілей і стратегій, пов'язаних з ІТ, стратегіям організації.
MEA01 Відстежувати, оцінювати та аналізувати ефективність та відповідність	Забезпечити прозорість виконання та відповідності, а також сприяти досягненню цілей.
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.
MEA03 Відстежувати, оцінювати та аналізувати відповідність зовнішнім вимогам	Забезпечити дотримання організацією діючих зовнішніх вимог.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
• у колег, що працюють в організації;
• у керівництва;
• в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;

2401 Звітування (продовження)

3.3 Інші настанови (продовження)

- у професійних організаціях;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Відповідні докази	Міра довіри до доказів.
Достатні докази	Міра кількості доказів; обґрунтовують усі суттєві питання щодо цілей та обсягу аудиту. Дивіться визначення терміну «докази».
Незначне порушення	Порушення є незначним, якщо розсудлива особа, врахувавши ймовірність існування інших невиявлених порушень, може дійти висновку, що таке порушення індивідуально чи у поєднанні з іншими порушеннями є незначним для об'єкта перевірки. Якщо розсудлива особа не може дійти такого висновку щодо певного порушення, таке порушення є більше, ніж незначне.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

2402 Подальша діяльність

Ця настанова описана у наступних розділах:

1. Мета настанови та її зв'язок зі стандартами
2. Зміст настанови
3. Зв'язок зі стандартами і процесами COBIT 5
4. Термінологія
5. Дата набуття чинності

1. Мета настанови та її зв'язок зі стандартами

1.0 Вступ

Цей розділ роз'яснює:

1.1 Мету настанови
1.2 Зв'язок зі стандартами
1.3 Використання термінів «функція аудиту» та «фахівці»

1.1 Мета

1.1.1 Мета цієї настанови полягає у наданні фахівцям з аудиту та підтвердження довіри до ІС вказівок щодо відстеження за умови вжиття керівництвом відповідних своєчасних заходів щодо рекомендацій та аудиторських результатів, наведених у звітах.

1.1.2 Фахівці з аудиту та підтвердження довіри до ІС повинні враховувати цю настанову при визначенні того, як необхідно застосовувати стандарти та професійні судження на практиці, а також бути в змозі виправдати будь-які відхилення від них і, за необхідності, знайти додаткові настанови.

1.2 Зв'язок зі стандартами

1.2.1 Стандарт 1401 Звітування
1.2.2 Стандарт 1402 Подальша діяльність

1.3 Використання термінів

1.3.1 Далі за текстом:
- «функція аудиту та підтвердження довіри до ІС» іменуватиметься як «функція аудиту»;
- «фахівці з аудиту та підтвердження довіри до ІС» іменуватимуться як «фахівці».

2. Зміст настанови

2.0 Вступ

Розділ «Зміст настанови» структурований таким чином, щоб надати інформацію про такі ключові теми, пов'язані зі завданнями з аудиту та підтвердження довіри до ІС, як:

2.1 Процес подальшого контролю
2.2 Заходи, запропоновані керівництвом
2.3 Прийняття ризику незастосування корегуючих заходів
2.4 Процедури подальшої діяльності
2.5 Терміни і календарне планування подальшої діяльності
2.6 Характер та обсяг подальшої діяльності
2.7 Відстрочення подальшої діяльності
2.8 Формування відгуків про подальшу діяльність
2.9 Подальша діяльність фахівців згідно з рекомендаціями для зовнішнього аудиту
2.10 Звітування про подальшу діяльність

2.1 Процес подальшого контролю

2.1.1 Подальші перевірки, які здійснюють фахівці, є процесом визначення адекватності, ефективності та своєчасності вжитих керівництвом заходів щодо спостережень і рекомендацій, про які йдеться у звітах, у тому числі отриманих від зовнішніх аудиторів та інших осіб.

2.1.2 Необхідно встановити процес подальшого контролю для сприяння забезпеченню достатньої впевненості у тому, що кожен перегляд, здійснений фахівцями, надає оптимальні вигоди організації шляхом застосування узгоджених результатів таких переглядів у відповідності до обов'язків керівництва, або що (вище виконавче) керівництво визнає і приймає ризик відстрочення або неврахування запропонованих результатів та / або рекомендацій.

2.2 Заходи, запропоновані керівництвом

2.2.1 В рамках розгляду питань з організацією, що підлягає аудиту, фахівці повинні узгодити результати завдань з аудиту та, за необхідності, план заходів, націлених на покращення діяльності.

2.2.2 Фахівці повинні обговорювати з керівництвом запропоновані заходи щодо застосування або розгляду рекомендацій та аудиторських коментарів, наведених у звітах. Такі запропоновані заходи повинні надаватися фахівцям і фіксуватися у вигляді відгуків керівництва в остаточних варіантах

2402 Подальша діяльність (продовження)

2.2 Заходи, запропоновані керівництвом		звітів із зазначенням дати їх впровадження та / або здійснення.
	2.2.3	Якщо фахівці та організація, що підлягає аудиту, дійшли згоди щодо запропонованих заходів, фахівці повинні розпочати процедури подальших перевірок згідно із параграфом 2.4.
2.3 Прийняття ризику незастосування корегуючих заходів	2.3.1	(Вище виконавче) керівництво може вирішити прийняти ризик невиправлення проблем, про які йдеться у звітах, у зв'язку з вартістю, складністю корегуючих заходів або іншими факторами, які необхідно враховувати. Необхідно інформувати керівну раду (або осіб, відповідальних за корпоративне управління) про рішення (вищого виконавчого) керівництва стосовно всіх значущих спостережень і рекомендацій, пов'язаних із завданнями, щодо яких керівництво приймає ризик невиправлення ситуації, про яку йдеться у звіті.
	2.3.2	Якщо фахівці вважають, що організація, що підлягає аудиту, взяла на себе такий рівень залишкових ризиків, який є неприйнятним для організації, вони повинні обговорити таке питання з керівництвом аудиту та підтвердження довіри до ІС і вищим виконавчим керівництвом. Якщо фахівці все ж не погоджуються з рішенням стосовно залишкових ризиків, разом з вищим виконавчим керівництвом вони повинні звітувати про таке керівної раді (або особам, відповідальним за корпоративне управління), щоб вирішити всі питання.
	2.3.3	Вище виконавче керівництво повинно документально оформляти та офіційно затверджувати прийняття ризиків і звітувати про таке особам, відповідальним за корпоративне управління.
2.4 Процедури подальшої діяльності	2.4.1	Необхідно встановлювати процедури подальших перевірок, а саме: • часові рамки на отримання відгуку керівництва щодо узгоджених рекомендацій; • оцінювання відгуків керівництва; • за необхідності, підтвердження відгуків (деталі наведено у параграфі 2.6); • за необхідності, подальшу діяльність; • процедуру звітування, яка передає спірні незадовільні відгуки та / або заходи на розгляд відповідного рівня керівництва та осіб, відповідальних за корпоративне управління; • процес прийняття на себе керівництвом супутніх ризиків у випадку відстрочення або невжиття корегуючих заходів.
	2.4.2	Автоматизована система відстеження і бази даних можуть сприяти здійсненню подальшої діяльності.
	2.4.3	Фактори, які необхідно враховувати при визначенні належних процедур подальшої діяльності: • важливість і вплив результатів і рекомендацій; • будь-які зміни середовища ІС, які можуть впливати на важливість і вплив результатів і рекомендацій; • складність виправлення ситуації, про яку йдеться у звіті; • час, витрати і зусилля, необхідні для виправлення ситуації, про яку йдеться у звіті; • наслідки невиправлення ситуації, про яку йдеться у звіті.
	2.4.4	Відповідальність за подальші заходи, звітування та передачу вирішення проблем на вищий рівень визначається у статуті аудиту.
2.5 Терміни і календарне планування подальшої діяльності	2.5.1	При визначенні термінів подальшої діяльності необхідно враховувати значущість результатів, про які йдеться у звітах, та наслідки невжиття корегуючих заходів. Визначення термінів подальшої діяльності відносно початкового звітування є питанням професійних суджень, що залежать від низки факторів, які необхідно враховувати, наприклад, від характеру або розміру супровідних ризиків для організації та вартості.
	2.5.2	Подальша діяльність, яка є невід'ємною частиною процесу аудиту ІС, повинна плануватися разом з іншими кроками, необхідними для здійснення кожного перегляду. На подальшу діяльність і терміни відповідних заходів, які встановлюються після їх узгодження з керівництвом, може впливати ступінь складності, ризики і пов'язані з ними впливи, результати перегляду, час, необхідний для застосування корегуючих заходів тощо.
	2.5.3	Узгоджені результати, пов'язані з питаннями з високим рівнем ризиків, необхідно контролювати після настання дати впровадження відповідних заходів. Їх відстеження може здійснюватися безперервно.
	2.5.4	Втілення всіх відгуків керівництва необхідно контролювати регулярно (наприклад, щоквартально), об'єднуючи різні завдання з аудиту, навіть якщо дати їх впровадження, яких дотримується

2402 Подальша діяльність (продовження)

2.5 Терміни і календарне планування подальшої діяльності (продовження)		керівництво, різняться. Інший підхід полягає у контролюванні окремих відгуків керівництва згідно з датою їх впровадження, узгодженою керівництвом.
2.6 Характер та обсяг подальшої діяльності	2.6.1	Як правило, організація, що підлягає аудиту, отримує часові рамки на надання відгуків, описуючих заходи, вжиті при виконанні рекомендацій.
	2.6.2	Відгуки керівництва, які детально описують вжиті заходи, повинні, за необхідності, оцінюватися фахівцями, що проводили початкову перевірку. По можливості, необхідно отримати аудиторські докази вжитих заходів.
	2.6.3	Якщо керівництво надає інформацію про заходи, вжиті при виконанні рекомендацій, а фахівці піддають сумніву таку інформацію або ефективність вжитих заходів, необхідно застосувати відповідні процедури перевірки або інші аудиторські процедури для підтвердження реального стану або статусу до формування висновків про подальшу діяльність.
	2.6.4	В рамках подальшої діяльності фахівці повинні оцінювати придатність невиконаних рекомендацій або рівень їх значущості. Фахівці можуть вирішити, що виконання певних рекомендацій вже недоречне. Така ситуація може мати місце за умови зміни прикладних програмних систем, застосування контролів відшкодувань або зміни бізнес-цілей або пріоритетів, коли початкові ризики фактично виключаються або значним чином зменшуються. Таким же чином, зміни середовища ІС можуть збільшити значущість впливів попередніх спостережень і потребу їх усунення.
	2.6.5	Може виникнути необхідність створення календарного плану завдань подальшої діяльності для підтвердження застосування критичних та / або важливих заходів.
	2.6.6	Фахівці повинні інформувати відповідний рівень керівництва про свої професійні судження щодо незадовільних відгуків або заходів керівництва.
2.7 Відстрочення подальшої діяльності	2.7.1	Фахівці несуть відповідальність за календарне планування подальшої діяльності при плануванні роботи. Календарне планування подальшої діяльності повинно ґрунтуватися на ризиках і пов'язаних з ними впливах, а також на ступені складності та часових затратах, необхідних для застосування корегуючих заходів.
	2.7.2	Також можуть виникати ситуації, коли фахівці роблять висновок, що усні чи письмові відгуки керівництва свідчать про достатність вжитих заходів у порівнянні з відносною важливістю спостережень чи рекомендацій щодо відповідних завдань. У таких випадках може виникнути необхідність у фактичній подальшій діяльності з перевірки в рамках наступних завдань, пов'язаних з відповідною системою чи питанням.
2.8 Формування відгуків про подальшу діяльність	2.8.1	Найбільш ефективними є письмові відгуки керівництва про подальші перевірки, оскільки вони сприяють підтвердженню та посиленню відповідальності керівництва за подальші заходи і досягнутий прогрес. Окрім того, письмові відгуки забезпечують точне фіксування заходів, обов'язків і поточного статусу. Фахівці можуть отримувати та фіксувати також і усні відгуки, які, по можливості, повинно затверджувати керівництво. Відгуки можуть також містити підтвердження заходів або виконання рекомендацій.
	2.8.2	Фахівці повинні робити запити та / або отримувати періодичні звіти від керівництва, відповідального за впровадження узгоджених заходів, з метою оцінювання досягнутого керівництвом прогресу, особливо в питаннях з високим рівнем ризиків і довготривалих корегуючих заходах.
2.9 Подальша діяльність фахівців згідно з рекомендаціями для зовнішнього аудиту	2.9.1	Залежно від обсягу та тривалості завдань з аудиту при здійсненні подальших перевірок згідно з відповідними стандартами аудиту ІС зовнішні фахівці можуть покладатися на узгоджені рекомендації внутрішніх фахівців. Обов'язки, пов'язані з такою подальшою діяльністю, визначаються у статуті аудиту або контракті.

2402 Подальша діяльність (продовження)

2.10 Звітування про подальшу діяльність

2.10.1 Звіти про статус виконання узгоджених корегуючих заходів, що ґрунтуються на звітах про завдання з аудиту та містять інформацію про невиконані узгоджені рекомендації, необхідно відправляти відповідному рівню керівництва та особам, відповідальним за корпоративне управління (наприклад, аудиторському комітету).

2.10.2 Якщо в рамках виконання наступних завдань з аудиту фахівці виявляють фактичне невиконання корегуючих заходів, про які керівництво звітувало як про «виконані», вони повинні повідомити про таке відповідний рівень керівництва та осіб, відповідальних за корпоративне управління. За необхідності, фахівці повинні отримати план поточних корегуючих заходів і планові дати їх застосування.

2.10.3 Після застосування всіх узгоджених корегуючих заходів необхідно відправити вищому виконавчому керівництву та особам, відповідальним за корпоративне управління, звіт, який детально описує всі вжиті та / або завершені заходи.

3. Зв'язок зі стандартами і процесами COBIT 5

3.0 Вступ

Цей розділ розглядає наступні питання:

3.1 Зв'язок зі стандартами

3.2 Зв'язок із процесами COBIT 5

3.3 Інші настанови

3.1 Зв'язок зі стандартами

Таблиця розглядає:

- найбільш придатні стандарти ISACA щодо аудиту та підтвердження довіри до ІС, які безпосередньо стосуються цієї настанови ;
- положення стандартів, які є найбільш придатними для цієї настанови.

Примітка. Нижче наведено тільки ті положення стандартів, які є придатними для цієї настанови.

Назва стандарту	Відповідні положення стандарту
1401 Звітування	Фахівці з аудиту та підтвердження довіри до ІС повинні звітувати про результати виконаних завдань, включаючи: • ідентифікацію організації, припустимого одержувача та будь-які обмеження щодо змісту та розповсюдження; • обсяг, цілі та період виконання завдань, а також характер, визначення терміну проведення та обсягу роботи, що підлягає здійсненню; • результати, висновки та рекомендації; • будь-які кваліфікації фахівців з аудиту та підтвердження довіри до ІС чи обмеження обсягу робіт, що стосуються виконання завдань; • підпис, дату та розповсюдження згідно з умовами статуту аудиту та контракту. Фахівці з аудиту та підтвердження довіри до ІС повинні гарантувати, що наведені в аудиторському звіті результати ґрунтуються на достатніх та відповідних аудиторських доказах.
1402 Подальша діяльність	Фахівці з аудиту та підтвердження довіри до ІС повинні виконувати відстеження відповідної інформації, щоб зробити висновок, чи керівництво своєчасно запланувало / вжило необхідні заходи для розгляду результатів та рекомендацій аудиторського звіту.

3.2 Зв'язок із процесами COBIT 5

Таблиця розглядає наступні питання:

- Процеси COBIT 5
- Цілі процесів COBIT 5

Окремі види діяльності, які здійснюються в рамках виконання цих процесів, містяться в «COBIT 5: Сприяння процесам».

2402 Подальша діяльність (продовження)

3.2 Зв'язок із процесами COBIT 5 (продовження)

Процес COBIT 5	Мета процесу
EDM01 Забезпечувати впровадження та підтримку основних положень корпоративного управління	Забезпечити єдиний підхід, інтегрований та узгоджений з підходом організації до корпоративного управління. Приймати такі рішення у сфері ІТ, які відповідатимуть стратегіям і цілям організації. Здійснювати ефективний та прозорий нагляд за процесами, пов'язаними з ІТ, та підтверджувати їх відповідність законодавчим і регуляторним вимогам, а також забезпечити дотримання членами керівної ради вимог до корпоративного управління.
EDM02 Забезпечувати отримання вигоди / переваги	Забезпечити оптимальний ефект від ініціатив, послуг та активів, пов'язаних з ІТ, економічно вигідні рішення та послуги, а також надійне і точне уявлення про витрати і можливі прибутки так, що потреби бізнесу задовольняються ефективно та продуктивно.
EDM03 Забезпечувати оптимізацію ризиків	Забезпечити, щоб ризики організації, пов'язані з ІТ, не перевищували рівень її схильності та піддатливості ризикам, вплив ризиків, пов'язаних з ІТ, на вартість організації визначений і контролюється, а потенціал відхилень, пов'язаних з невідповідностями, мінімізований.
MEA02 Відстежувати, оцінювати та аналізувати системи внутрішніх контролів	Забезпечити прозорість для ключових зацікавлених сторін щодо адекватності системи внутрішніх контролів та, відповідно, довіри до діяльності, впевненості у досягненні цілей організації та адекватного розуміння залишкових ризиків.
MEA03 Відстежувати, оцінювати та аналізувати відповідність зовнішнім вимогам	Забезпечити дотримання організацією діючих зовнішніх вимог.

3.3 Інші настанови

При застосуванні стандартів і настанов фахівцям рекомендується, за необхідності, звертатися до інших настанов. У сфері аудиту та підтвердження довіри до ІС їх можна знайти:
- у колег, що працюють в організації;
- у керівництва;
- в органах корпоративного управління організацією, наприклад, в аудиторському комітеті;
- у професійних організаціях;
- в інших професійних настановах (наприклад, у книгах, документах чи інших настановах).

4. Термінологія

Термін	Визначення
Подальші перевірки	Процес, за допомогою якого внутрішні аудитори оцінюють адекватність, ефективність і своєчасність вжитих керівництвом заходів щодо спостережень і рекомендацій, про які йдеться у звітах, у тому числі отриманих від зовнішніх аудиторів та інших осіб. Джерело: Інститут внутрішніх аудиторів – Методичні вказівки 2 500. A1-1; авторське право © належить корпорації «Інститут внутрішніх аудиторів». Усі права захищено.
Професійні судження	Застосування відповідних знань та досвіду при інформованому прийнятті рішень про напрямки дій, що відповідають обставинам завдань з аудиту та підтвердження довіри до ІС.

5. Дата набуття чинності

5.1 Дата набуття чинності

Ця переглянута настанова є чинною для всіх завдань з аудиту та підтвердження довіри до ІС з або після 1 вересня 2014 року.

3. Інструментарій і методики аудиту та підтвердження довіри до ІС

Інструментарій і методики забезпечують фахівців з аудиту та підтвердження довіри до ІС додатковими прикладами.

Цей розділ містить посилання на джерела ISACA, а також на інші відповідні та надійні джерела.
- Аналітичні записки: www.isaca.org/whitepapers (безкоштовні PDF-файли).
- Програми аудиту / підтвердження довіри до: www.isaca.org/auditprograms (безкоштовні файли Word для членів ISACA).
- Сімейство продуктів COBIT 5: www.isaca.org/cobit.
- Серія технічних довідників і довідників з управління ризиками: www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/Pages/Reference-Series.aspx (доступні у книгарні ISACA).
- Колонки журналу IT Audit Basics[15]: www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/IT-Audit-Basics/Pages/IT-Audit-Basics-Articles.aspx (безкоштовний доступ).

Перелік усіх результатів досліджень ISACA наведено на наступній сторінці: www.isaca.org/Knowledge-Center/Research/Pages/All-Deliverables.aspx.

Додаткову інформацію щодо окремих видань ISACA можна отримати на наступній сторінці: www.isaca.org/bookstore, або звернувшись за електронною адресою: bookstore@isaca.org.

[15] IT Audit Basics – «Основи аудиту IT»

Форма для подання коментарів

Ми зацікавлені в отриманні Ваших відгуків щодо ITAF і пропозицій щодо доповнень / виправлень. Будь ласка, вкажіть детальну інформацію щодо Ваших пропозицій та обґрунтування запропонованих виправлень. Надішліть Ваші коментарі на ім'я директора з розвитку професійних стандартів факсом: +1 847 253 1443, електронною поштою: standards@isaca.org, або на адресу ISACA: Алгонквін Роуд, 3701, офіс 1010, Роллінг-Медоуз, Іллінойс, США, 60008.

ПІБ: _____

Організація: _____

Країна: _____ Електронна пошта: _____

Розділ: _____

Пропозиція щодо виправлень: _____

_____

_____

_____

_____

Обґрунтування виправлень: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Дякуємо!