ПРАКТИЧНА МЕТОДОЛОГІЯ ІТ-АУДИТУ

Зміст

1. Вступ: актуальність IT-аудиту, завдання IT-аудитора

В умовах стрімкого розвитку інфраструктури та поглиблення інформатизації господарських процесів ефективність діяльності підприємств, установ та організацій дедалі більше залежить від інформаційних технологій (ІТ), що використовуються в системах управління. Нині середовище інформаційних технологій (ІТ-середовище) як структурна складова організації являє собою складну систему, яка об'єднує різноманітні інформаційні, програмні, технічні, людські й інші види ресурсів для досягнення цілей організації, підприємства, установи. Це зумовлює зростання потреби у підвищенні ефективності й економічності використання ІТ, збільшення переваг і усунення недоліків від їх застосування, а також обгрунтування витрат на ІТ. Для задоволення такої потреби все більшого значення набуває регулярне застосування в системі управління організацій аудиту інформаційних технологій (ІТ-аудиту).

ІТ-аудити є ключовим компонентом для забезпечення якості інформаційних систем та прикладного програмного забезпечення. Без надійних інформаційних систем та результативних ІТ-заходів контролю, організація не взмозі правильно виконувати операції/транзакції та узагальнювати надійну фінансову звітність, що, своє чергою, впливає на рівень досягнення поставлених перед нею завдань та цілей.

Що персонально дає ІТ-аудит?

Керівнику
- розуміння проблем і шляхів їх вирішення
- відповідність ІТ планам розвитку організації
- регламентацію процесів
- оптимізацію бюджету і збереження інвестицій в ІТ

ІТ-департаменту
- виявлення проблем і вузьких міст системи
- план розвитку ІТ
- підтримка керівництва для впровадження новинок

Працівникам
- регламентація діяльності
- розуміння напрямку розвитку процесів
- розуміння цілей впровадження ІТ
- стабільна робота

Даний посібник з ІТ-аудиту розроблений для надання вказівок щодо методологічних та практичних аспектів проведення внутрішнього ІТ-аудиту.

У міжнародних стандартах професійної практики внутрішнього аудиту,

схвалених Інститутом внутрішніх аудиторів (ІВА), велика увага приділяється ризикам, пов'язаним з ІТ-середовищем. У 2009 році ці стандарти оновлено наступними обов'язковими аспектами:

1210.A3 – Внутрішні аудитори повинні мати достатні знання про ключові ризики та контролі інформаційних технологій, а також про доступні технологічні методи аудиту для виконання своєї роботи. Однак, не очікується, що всі внутрішні аудитори повинні мати компетентність внутрішнього аудитора, головним обов'язком якого є аудит інформаційних технологій.
2110.A2 – Функція внутрішнього аудиту повинна оцінювати, чи сприяє управління інформаційними технологіями організації реалізації стратегій та цілей організації.

Слід зауважити, що користувачам цього посібника необхідно мати достатній рівень знань про процес внутрішнього аудиту в українських державних установах[1].

Завдання ІТ-аудитора

Кваліфікований ІТ-аудитор повинен надавати об'єктивну оцінку та поради (рекомендації) щодо *аспектів якості ІТ*[2].

Оцінка та поради (рекомендації) охоплюють наступні аспекти ІТ:

- Інформаційна стратегія
- Інформаційне управління та інформаційна технологія
- Інформаційні системи
- Технічні системи
- Системи обробки
- Операційна підтримка

Професія ІТ-аудитора вимагає спеціального досвіду у сфері інформаційних технологій та з питань забезпечення організації управлінською інформацією. ІТ-аудитори повинні бути ознайомлені із загальноприйнятими методами і прийомами внутрішнього аудиту, в т. ч. з тими, які використовуються під час ІТ-аудиту, тестуванням та оцінкою ризиків, пов'язаних з ІТ. Вони також повинні володіти інформацією про вартість ІТ та спеціальними навичками у деяких сферах прикладного програмного забезпечення. Збільшення актуальності ІТ посилює вимоги до якості, яка очікується від ІТ-аудиторів при виконанні завдань.

[1] коротко процес аудиту описано в розділі 5 цього посібника (детальний опис загального процесу міститься у Методологічних вказівках з внутрішнього аудиту для державного сектору України).
[2] детально у розділі 3.2 цього посібника.

2. IT-аудит: термінологія і визначення

У цьому розділі описується спеціальна термінологія IT-аудиту та визначення відповідно до міжнародних стандартів та правил.

IT-аудит[3] - це незалежна і неупереджена оцінка надійності, безпеки (включаючи безпеку персональних даних), результативності та ефективності автоматизованих інформаційних систем, організації департаменту з автоматизації, технічно-організаційної інфраструктури обробки автоматизованої інформації. Ця діяльність поширюється як на діючі операційні системи, так і на системи, які розробляються.

Термін	Визначення[4]
База даних	Збережений набір пов'язаних даних, необхідних організаціям та особам для задоволення їхніх потреб в обробці та видачі інформації
Безпека	Здатність системи до захисту інформації та ресурсів системи із врахуванням конфіденційності та цілісності
Дизайн	План, опис або графічне зображення, метою якого є наочне представлення IT заходів контролю, процесу чи іншого об'єкту аудиту. Дизайн, як правило, розробляється до впровадження заходів контролю та розробки інформаційної системи.
Загальний контроль	Захід контролю, відмінний від контролю за прикладними програмами, пов'язаний із середовищем, у якому розробляються, підтримуються та функціонують прикладні системи на основі комп'ютерних технологій, а тому застосовується до усіх видів прикладних програм. Цілі загального контролю полягають у гарантуванні належної розробки та впровадження прикладних програм, а також цілісності програми, файлів даних і комп'ютерних операцій. Як і заходи контролю за прикладними програмами, загальні заходи контролю можуть бути як ручними, так і автоматизованими. Приклади загальних заходів контролю включають розробку і впровадження стратегії інформаційних систем, політики безпеки інформаційних систем, організації персоналу інформаційних систем для розподілу конфліктних обов'язків, а також планування запобігання збоям та відновлення системи.
Інформаційні системи	Сукупність стратегічних, управлінських та операційних видів діяльності, пов'язаних зі збором, обробкою, збереженням, розповсюдженням та використанням інформації, та відповідних технологій.
IT-інфраструктура	Комплекс апаратного, програмного забезпечення та засобів, які об'єднують IT-активи установи, зокрема обладнання (в тому числі

[3] визначення, яке використовується „Norea" – голландською асоціацією IT-аудиторів.

[4] визначення ISACA (Асоціація аудиту та контролю інформаційних систем). Більше визначень на http://www.isaca.org/Pages/Glossary.aspx

	сервери, рутери, мережеві комутатори та кабелі), програмне забезпечення, послуги та продукти, які використовуються для зберігання, обробки, передачі та видачі усіх форм інформації для користувачів установи.
Контроль на рівні прикладної програми	Правила, процедури та заходи, призначені надавати помірковану гарантію щодо досягнення цілей, пов'язаних із даним автоматизованим рішенням (прикладною програмою)
Критерії аудиту	Стандарти і рамки, які використовуються для вимірювання та презентації предмета дослідження, за якими ІТ-аудитор його оцінює
Надійність	Здатність системи чи компонента реалізувати визначені функції за визначених умов та період часу
Мережа	Система пов'язаних між собою комп'ютерів та комунікаційного обладнання
Операційна ефективність	Функціонування об'єкту, що був розроблений у визначений період часу
Прикладне/програмне забезпечення	Комп'ютерна програма або набір програм для обробки записів у рамках виконання конкретної функції
Розподіл обов'язків (РО)	Базовий захід внутрішнього контролю, який запобігає або виявляє помилки і порушення шляхом покладання на одних осіб відповідальності за ініціювання і запис транзакцій, а на інших – за збереження активів. Примітка: Розподіл обов'язків зазвичай використовується у великих ІТ організаціях, аби одна єдина особа не могла непомітно проводити шахрайські чи зловмисні операції.
Ціль аудиту	Конкретна ціль (цілі) аудиту: надати висновок/висновки і, якщо необхідно, рекомендації для покращення управління ІТ-заходами та засобами. Крім того, ціль ІТ-аудиту може полягати у наданні поміркованої гарантії щодо відсутності недоліків в інформаційних об'єктах або не фінансовій інформації.
Шкідливі програми	Призначені проникати, пошкоджувати або діставати інформацію з комп'ютерної системи без згоди власника.

3. Об’єкти IT-аудиту

У цьому розділі описано різні об’єкти, на яких може зосереджуватися IT-аудит. Спочатку пояснено зміст об’єкта та межі IT-аудиту. Потім описано аспекти якості об’єктів IT та їхні найпоширеніші види. Завершено розділ міжнародно прийнятим розподілом видів заходів контролю, пов’язаних з IT.

3.1 Об’єкт та межі IT-аудиту

Об’єкт IT-аудиту (предмет дослідження) слід описувати таким чином, щоб не виникало непорозумінь щодо визначення його меж. Належний об’єкт IT-аудиту можна ідентифікувати, оцінювати однаковим способом або за визначеними критеріями аудиту[5], і він носить такий характер, що інформація про нього може стати предметом процедур збору достатніх належних доказів для формування висновку.

Проведення аудиту IT-середовища організації, а відповідно визначення правильного об’єкта IT-аудиту та критеріїв аудиту, слід базувати на ризиках. IT-аудитори повинні вирішувати, які сфери підлягають аудиту на основі оцінки ризиків шляхом визначення критичних[6] активів IT та врахування потенційних ризиків і важливих заходів контролю. Активи – це цінні інформаційні системи, процедури і правила. Ризики – це потенційно «погані події», які можуть відбутися з активами. Заходи контролю – це пом’якшуючі фактори для захисту активів від потенційних ризиків.

Деякі типові фактори ризику для інформаційних технологій можуть включати:

- характер інформаційної системи, напр., з використанням Інтернету чи ні. Або чи це критична фінансова система чи базова реєстраційна система;
- складність інформаційної системи, напр., чи це проста незалежна система чи ланка ланцюжка взаємозалежних систем;
- зрілість інформаційної системи, напр., чи це нова система з багатьма питаннями, які можуть виникнути вперше, чи це зріла система, яку

[5] Критерії аудиту наведені у розділі 4 цього посібника та в додатку до нього.
[6] Критичні, означає ті, IT активи, які є критично важливі для організації, оскільки помилки можуть мати серйозні наслідки, такі як великі фінансові втрати, значна шкода середовищу, нанесення шкоди здоров’ю чи життю людини (напр. госпіталізація). Синонімом до слова «критичні» є «ключові».

вже неодноразово перевіряли аудитом;

- вартість інформаційної системи часто пов’язана із складністю інформаційної системи. Актуальна у тому контексті, що дуже дорогі системи привертають більше уваги вищого керівництва;
- вразливість і захист персональних даних, напр., інформація у медичній системі вразливіша за інформацію у фінансовій системі;
- аспекти безперервності, напр., деякі інформаційні системи повинні постійно функціонувати, тоді як інші – тільки у робочий час.

Межі ІТ-аудиту означають:

- аспекти якості, які треба оцінити (конфіденційність, цілісність систем або даних, доступність, результативність, ефективність, дотримання законів і постанов, тощо). Ці аспекти якості пояснюються у підрозділі 3.3;
- рівень ІТ-аудиту: результативність структури і/або операційна результативність. Пояснення наведено нижче.

Результативність структури передбачає оцінку того, чи ІТ-заходи контролю належно розроблені для запобігання чи виявлення ризиків. Заходи контролю розроблені неефективно, якщо деяких заходів бракує або якщо запроваджені заходи контролю не досягають відповідної цілі контролю. У загальному, дизайн[7] задокументований у правилах ІТ, правилах безпеки, планах та процедурах безпеки, тощо.

Приклади типових запитань (критеріїв аудиту) для розгляду структури такі[8]:

1. Визначити, чи існує таблиця розподілу обов’язків (РО) і розглянути її на предмет адекватного розподілу ключових обов’язків.
2. Запитати та підтвердити, чи існують задокументовані процедури для виправлення існуючих помилок.
3. Дістати інформацію про функціональний опис та структуру введення даних про транзакції. Перевірити функціональність та структуру на предмет наявності своєчасних і вичерпних перевірок та повідомлень про помилки.

Операційна результативність передбачає оцінку реалізації ІТ-заходів контролю у певний часовий проміжок відповідно до структури. Це означає, що ІТ-аудитор повинен провести кілька тестів для перевірки дієвості ІТ-заходу контролю у визначеному часовому проміжку. Для охоплення усього періоду часу ІТ-аудитор повинен зібрати, узагальнити і оформити у файл докази про різні моменти у визначеному часовому періоді, щоб бути помірковано

[7] визначення "дизайну" надано у розділі 2 цього посібника.

[8] Приклади щодо дизайну та операційної результативності взяті із Загальної програми аудиту/гарантії прикладних програм. Більше інформації про цю програму наведено у додатку.

упевненим у тому, що ІТ-захід контролю функціонував ефективно протягом усього часового проміжку.

Приклади типових запитань (критеріїв аудиту) для розгляду операційної результативності такі:

1. Перевірити документи, відстежити транзакції усього процесу і, за можливості, використовувати автоматизований збір доказів, у тому числі дані вибірки, інтегровані аудиторські модулі або CAATT[9], відстежити транзакції підтвердження ефективності заходів контролю щодо надання авторизованого доступу.
2. Запитати та підтвердити, що повідомлення про помилки збираються і своєчасно передаються, транзакції не проводяться, поки не виправлені або належним чином прийняті внесені помилки, які не можна одразу виправити, тоді як продовжується обробка чинних транзакцій, і що записи про помилки переглядаються та враховуються у визначений та розумний (прийнятний) період часу.
3. Зробити вибірку процесів вводу джерел даних. Запитати та підтвердити наявність механізмів, які забезпечують реалізацію процесів вводу джерел даних відповідно до визначених критеріїв своєчасності, повноти і точності.

3.2 Аспекти якості

ІТ-аудитор оцінює один чи більше аспектів якості об’єктів аудиту, в т.ч. управління ІТ процесом. Найбільш поширеними аспектами якості в ІТ-аудиті є:

Надійність

У загальному надійність можна визначити як вірогідність того, що інформаційна система на задовільному рівні виконає завдання, для якого її було розроблено або задумано, за певний період часу у визначеному середовищі. Для ІТ-аудитів надійність розділено на три аспекти (визначення ISACA):

1. Конфіденційність (ексклюзивність) – збереження обмежень з авторизації доступу і розкриття даних, включаючи засоби для захисту особистих даних і конфіденційної інформації.
2. Цілісність системи або даних полягає у повноті, правильності і точності. Захист від неналежної зміни інформації або її знищення, а також включає забезпечення неспростовною і справжньою інформацією.
3. Доступність (безперервність) – забезпечення своєчасним і надійним доступом до інформації та її використання.

[9] детально про CAATT у підрозділі 4.4. цього посібника.

Безпека (інформації)[10] означає захист інформації та інформаційних систем від неавторизованого доступу або зміни інформації, яка зберігається, обробляється чи передається, а також відмови у послузі не авторизованим користувачам. Безпека інформації передбачає заходи, необхідні для виявлення, документування та боротьби з такими загрозами.

Результативність – це здатність досягнути бажаного результату.

Ефективність означає виконання або здатність виконати завдання у співвідношенні із затратами часу і ресурсів.

3.3 Типові для державних установ види IT-аудиту

Існує багато видів IT-аудитів. Найбільш поширені IT-аудити такі:

a) IT-аудит безпеки (конфіденційність, цілісність і доступність): Ідеться не тільки про безпеку інформації у системі чи прикладній програмі, а й також про те, як організована безпека інформації, цілісність систем та розподіл відповідальності в державній установі. Для цього виду аудиту часто використовується Основа ISO/IEC 27001, але також можуть бути корисними COBIT5, GTAG-8 і Загальна програма аудиту/гарантії прикладних програм[11].

b) IT-аудит якості (результативність, ефективність): У цьому IT-аудиті розглядається якість інформаційної системи, прикладної програми або/і бізнес процесів. Можуть бути корисними COBIT5, GTAG-8 і Загальна програма аудиту/гарантії прикладних програм. Залежно від виду IT-організацій, також можуть бути корисними ITIL, BiSL або ASL.

c) Аудит IT-проекту, під час якого внутрішній аудитор перевіряє управління та організацію IT-проекту, наприклад, запровадження інформаційної системи. Важливими аспектами для оцінки є: організація проекту, планування, персонал і його обов'язки, кошти, час, управління діяльністю та змінами. Найбільше підходить для цього виду основа PRINCE2.

d) Аудит розробки систем: аудит для перевірки, чи системи, які розробляються, відповідають цілям організації, та для гарантії того, що системи розробляються відповідно до загально прийнятих стандартів розробки систем. Використовуються такі самі основи, як у b.

e) Аналіз даних: не зовсім IT-аудит, але часто це частина фінансового аудиту. IT-аудитор може виконувати функцію підтримки в аналізі фінансових даних. Завдання IT-аудитора полягає у виокремленні та зборі фінансової

[10] Надійність стосується внутрішнього функціонування системи, в той час як безпека означає зовнішні атаки непередбачуваних сторін. Помилки у безпеці зумовлять вплив на надійність. Тому якісні ознаки, такі як конфіденційність, цілісність і доступність також характерні і для безпеки IT аудиту.

[11] Основи пояснені в додатку.

інформації з бази даних інформаційної системи, у запитах та звітах, необхідних для аналізу фінансових даних. У наступному розділі наведені корисні інструменти для проведення аналізу даних. Аналіз даних вимагає ретельної підготовки, враховуючи бажаний результат, наявність та можливості даних.

Взагалі існує багато думок щодо класифікації функціональних видів IT-аудитів. Зокрема, виділяють ще такі види:

Аудит заходів контролю (controls review) – детальна перевірка ручних й автоматизованих заходів контролю з метою оцінки рівня достовірності виконаних транзакцій і звітів, що були згенеровані відповідними системами;

Судовий аудит (forensic audit) – аудит, що проводиться у випадку підозр у шахрайстві, незаконних діях або порушеннях політики і правил, затверджених в організації. Збір аудиторських доказів здійснюється за допомогою застосування відповідних засобів для відновлення захисту від таких пристроїв, як кишенькові електронні помічники (PDAs), мобільні телефони тощо, які можуть бути використані для незаконних дій.

При цьому, слід звернути увагу на те, що окремо IT-аудит проводиться дуже рідко. Як правило, він є елементом аудиту ефективності.

3.4 IT-заходи контролю: загальні заходи контролю і заходи контролю за прикладними програмами

Розрізняють дві широкі групи заходів контролю інформаційних систем, зокрема:

a) Загальні заходи контролю;
b) Заходи контролю за прикладними програмами.

Ці заходи контролю також оцінюються під час IT-аудиту.

Загальні заходи контролю

Цілі загальних заходів контролю полягають у належній розробці та впровадженні прикладних програм, а також у цілісності програм, файлів даних і комп'ютерних операцій. Ці процеси використовує функція IT для управління та контролю IT-середовища (персонал, процеси і технології). Загальні IT-заходи контролю забезпечують упевненість в тому, що IT-процес триває у часі послідовно.

Загальні заходи контролю стосуються структур, правил і процедур, які регулюють усю або головні частини інформаційної системи установи, такі як: комп'ютер, головний сервер, мережа та налаштування кінцевих користувачів. Загальні заходи контролю створюють середовище контролю, в якому функціонують прикладні системи.

Головні категорії загальних заходів контролю такі:

a) Планування і управління програмою безпеки: забезпечує рамкові основи та безперервний цикл заходів для управління ризиками, розробки правил безпеки, делегування обов'язків і моніторингу ефективності заходів контролю;

b) Заходи контролю щодо функціонування центру даних: напр., заходи контролю щодо придбання і впровадження системного програмного забезпечення та засобів телекомунікаційного програмного забезпечення; програмного забезпечення графіку робіт, дій операторів, баз даних (процедури створення резервної копії даних та їх відновлення);

c) Заходи контролю щодо безпеки доступу: заходи контролю, які запобігають неналежному і неавторизованому використанню інформаційної системи;

d) Заходи контролю щодо обслуговування систем: заходи контролю щодо методології розробки, в тому числі структури інформаційної системи, вимог до документації, управління змінами;

e) Розподіл обов'язків стосується правил, процедур та управлінської структури для управління та контролю з покладанням на різних осіб відповідальності за ініціювання та запис транзакцій.

Заходи контролю за прикладними програмами

Заходи контролю за прикладними програмами стосуються різних та спеціальних структур, правил і процедур, які безпосередньо пов'язані з конкретними прикладними програмами та призначені контролювати обробку даних.

Ціль заходів контролю за прикладними програмами полягає у забезпеченні того, що:

- Введення даних є точним, вичерпним, авторизованим і правильним;
- Дані обробляються належним чином у прийнятний часовий проміжок;
- Збережені дані точні та вичерпні;
- Видані дані точні та вичерпні;
- Записується процес проходження даних від вводу до зберігання, і до можливої видачі.

Найбільш важливі заходи контролю за прикладними програмами такі:

- Заходи контролю щодо вводу – використовуються здебільшого для перевірки цілісності даних, які вводяться в прикладну бізнес-програму як безпосередньо персоналом, так і віддалено бізнес-партнером, або через веб-інтерфейс, або прикладну програму з Інтернет-доступом. Введення даних

перевіряється, щоб забезпечити його відповідність визначеним параметрам.

- Заходи контролю щодо обробки даних – забезпечують автоматизованим засобом гарантії вичерпної, точної і авторизованої обробки даних.
- Заходи контролю щодо видачі даних – охоплюють результат обробки даних і мають порівнювати результати видачі із запланованим результатом, перевіряючи видані дані із введеними даними.
- Заходи контролю щодо цілісності – здійснюють моніторинг даних, які обробляються і зберігаються для забезпечення їхньої узгодженості та правильності.
- Управлінський слід – обробка історії заходів контролю, яка дає керівництву можливість визначати транзакції та події, які записуються шляхом відстеження транзакцій від джерела до видачі даних та у зворотному порядку. Ці заходи контролю також здійснюють моніторинг результативності інших заходів контролю та виявляють помилки якнайближче до джерел їх виникнення.

Заходи контролю за прикладними програмами більш надійні ніж ручні. Людський фактор при застосуванні ручних заходів контролю приводить до відхилень. Заходи контролю на вході перевіряють правильність введених даних, автоматизовані заходи контролю у той же самий спосіб перевіряють цілісність і правильність. Якщо у прикладній програмі не застосовуються заходи контролю взагалі або застосовуються в обмеженому обсязі, IT-аудитору слід порекомендувати заходи контролю (в т.ч. за необхідністю – додаткові) за прикладними програмами з огляду на їх надійність та контроль за усім процесом. Після запровадження заходу контролю за прикладною програмою, якщо внесено мало змін у прикладну програму, базу даних або технологію, організація може покладатися на цей захід контролю до внесення суттєвих змін.

4. Критерії, основи та інструменти аудиту

У цьому розділі надається підтримка IT-аудитору у підготовці набору критеріїв аудиту, використанні рамкових основ та інструментів, пов'язаних з IT-аудитом.

4.1 Критерії аудиту: норма, встановлена як інструмент для вимірювання

Для проведення IT-аудиту аудитору необхідний належний набір

критеріїв аудиту, які можна застосувати до об’єкта IT-аудиту. Критерії аудиту – це принципи (або норми), які використовуються для оцінки чи тестування об’єкта аудиту, та якщо необхідно для презентації або повідомлення результатів аудиту. Мета розробки набору критеріїв аудиту полягає у створенні набору норм для відображення реальності. Критерії аудиту узгоджуються з керівництвом.

Критерії аудиту вказують на об’єкт аудиту, як правило, це спеціально розроблена основа /робоча програма для IT-аудитора.

Набір критеріїв аудиту може бути поєднанням наступного:

- Наприклад такі *основи* , як COBIT5 (як правило витяг з неї);
- Вимога з внутрішнього положення або законодавства;
- Процес/правила/процедури організації IT процесу або їх частина.

Важливо, щоб IT-аудитор знав, що він повинен обрати правильні критерії аудиту на основі об’єкта IT-аудиту, його ризиків (абз. 3.2) та межі IT-аудиту. Зазвичай критерії аудиту походять з багатьох рамкових основ. Час, який IT-аудитор (і підрозділ аудиту) міг витратити на розробку власних основ для різних IT-об’єктів, він витрачає на аудит. При цьому IT-аудитор (і підрозділ аудиту) мають перевіряти, чи підходять обрані критерії аудиту для кожного нового IT-аудиту.

Визначення критеріїв аудиту

Критерії аудиту мають бути адаптовані до кожного окремого виду та об'єкта IT-аудиту. Критерії аудиту необхідні для послідовної оцінки або вимірювання об’єкта IT-аудиту для надання (професійного) аудиторського висновку. Без основи для порівняння, яка створюється адаптованими (обраними для IT-аудиту) критеріями аудиту, будь-який висновок не виключає можливості різного трактування та непорозуміння.

Критеріям IT-аудиту притаманні наступні характеристики:

- *актуальність:* критерії аудиту є актуальними, якщо вони відповідають діючій нормативно-правовій базі та середовищу IT-аудиту;
- *повнота*: критерії аудиту вичерпні, якщо не пропущено важливі фактори, які можуть вплинути на висновки у контексті завдання;
- *надійність*: надійні критерії аудиту дозволяють зробити помірковано послідовну оцінку або вимірювання об’єкта аудиту та обґрунтувати аудиторські висновки;
- *об’єктивність*: об'єктивні критерії оцінки сприяють наданню неупереджених висновків;
- *чіткість*: чіткі критерії аудиту сприяють наданню точних і однозначних висновків, які не допускають суттєво різного трактування.

ІТ-аудитор робить оцінку критеріїв аудиту для конкретного завдання, перевіривши їх відповідність вищенаведеним характеристикам. Відносна важливість кожної характеристики конкретного завдання – це питання професійного судження аудитора.

Керівництво ухвалює остаточне рішення, які критерії аудиту використовувати. Рівень залучення керівництва до визначення критеріїв аудиту може бути різним для кожного завдання:

- Низьким: можливо, керівництво вимагає використання стандартизованої тестової основи на базі загальноприйнятих норм або стандартів кращої практики;
- Високим: також можливо, що критерії аудиту становлять частину управлінської основи як такої, наприклад, у вигляді опису об’єкта аудиту/внутрішнього контролю в організації. У цьому випадку критерії аудиту базуються на аналізі ризиків самою організацією, можливо, враховуючи вимоги третіх сторін (таких як користувачі). ІТ-аудитор має перевірити до початку завдання, чи запропонований стандарт узгоджується з його основоположним ризиком та заявленими управлінськими цілями.

Загальні і спеціальні критерії аудиту

Критерії аудиту можуть бути загальними або спеціально розробленими. Загальні критерії аудиту передбачені законодавством або рішеннями уповноважених чи визнаних експертних органів, які дотримуються прозорого процесу. Спеціальні критерії аудиту розробляються для досягнення цілей завдання. Вибір загальних чи спеціальних критеріїв аудиту впливає на роботу, яку виконує аудитор для оцінки можливості застосування критеріїв аудиту для відповідного завдання.

Доступність критеріїв аудиту

Необхідно, щоб критерії аудиту були доступними для відповідних користувачів, щоб вони могли зрозуміти, як оцінювався або тестувався об’єкт ІТ-аудиту. Критерії аудиту стають доступними для відповідних користувачів шляхом:

- включення їх безпосередньо у звіт;
- вони можуть бути оприлюдненими;
- включення їх чітким способом у презентацію інформації про об’єкт ІТ-аудиту.

4.2 Основи ІТ-аудиту

Для обрання правильної основи ІТ-аудитор має вирішити, яка основа найбільш підходить по відношенню до ІТ-об’єкта. Наприклад:

- Якщо ІТ-об’єкт – це Безпека, то найкращий вибір - ISO/IEC 27001.
- Якщо ІТ-об’єкт – це Проект, то найкращий вибір - PRINCE 2.
- Якщо ІТ-об’єкт – це Заходи контролю за прикладними програмами, то найкращий вибір – це GTAG-8 або Загальна програма аудиту/гарантії прикладних програм.
- Якщо ІТ-об’єкт – це якість процесів ІТ-департаменту, тоді, ймовірно, ITIL – це найкраща основа.

Із цих основ (або з іншої основи за бажанням), ІТ-аудитор може вибрати необхідну та правильну інформацію для визначення критеріїв аудиту, у послідовності наступних кроків:

1. "Зрозуміти середовище": зібрати актуальну інформацію, щоб зрозуміти організацію та її ІТ-інфраструктуру, прикладні програми, ІТ-процеси, ІТ-організацію, тощо.
2. Визначити і класифікувати ризики, пов’язані з ІТ-об’єктом та обсяг ІТ-аудиту. Наприклад: якщо обсяг "безпека", то актуальні ризики - втрата конфіденційності, цілісності та доступності інформації. Та якщо, наприклад, "доступність" не охоплюється ІТ-аудитом, то відсутня необхідність робити наступний крок щодо доступності.
3. Обрати заходи контролю, які очікуються в ІТ-організації та ІТ-системі щодо ІТ- об’єкта. Це критерії аудиту, які використовуватиме аудитор.
4. Побудувати основу ІТ-аудиту з цими критеріями аудиту.

Основи (стандарти, норми), які використовуються під час проведення ІТ-аудиту:

- **COBIT 5**
- **ITIL V3**
- **PRINCE 2**
- **ASL**
- **BiSL**
- **ISO/IEC[12] 27001 і 27002**
- **Керівництво з аудиту глобальних технологій 8**
- **Загальна програма аудиту/гарантії прикладних програм**

ІТ-аудитору слід володіти достатніми знаннями щодо того, де їх застосовувати та які сфери вони охоплюють.

Більш детально про основи (стандарти), а також окремі приклади їх використання під час проведення внутрішнього аудиту наведено у додатку до цієї методології.

[12] Міжнародна організація зі стандартизації/Міжнародна електротехнічна комісія

4.3 Набір інструментів IT-аудиту для конкретних завдань

Інструменти аудиту стають дедалі важливішими для IT-аудитора. IT-середовища, прикладні програми, транзакції та інше настільки складні в наш час, що інструменти аудиту важливі для розуміння функціонування інформаційних систем. Для кожного IT-аудиту аудитор має вирішити, чи потрібні йому спеціальні інструменти і які саме. IT-аудитор має враховувати, чи він може проводити аудит щодо усіх актуальних аспектів об’єкта IT-аудиту і чи може виявити усі факти, не використовуючи інструментів.

Офіційна назва для спеціальних інструментів аудиту – Інструменти і прийоми комп'ютеризованої підтримки аудиту (CAATTs). Використання CAATTs означає, що IT-аудитор використовує комп’ютерні прикладні програми для автоматизації та сприяння IT-аудиту для обробки даних, важливих для аудиту, які містяться в інформаційній системі.

Застосування CAATTs допомагає забезпечити належне охоплення питань щодо огляду заходів контролю за прикладними програмами, особливо, коли під час тестового періоду мають місце тисячі або, можливо, мільйони транзакцій. У таких випадках було б неможливо дістати адекватну інформацію у форматі, який можна переглянути без використання автоматизованих інструментів.

Оскільки CAATTs дають можливість аналізувати великі обсяги даних, IT-аудит за підтримки CAATT тестування може провести повний огляд усіх транзакцій та виявити відхилення (напр., дублювання продавців або транзакцій) або набір заздалегідь визначених питань контролю (напр., розподіл обов'язків). Якщо CAATTs не використовуються, такий огляд доведеться робити шляхом вибірки, допускаючи вищий рівень невпевненості.

CAATTs також важливі для тестування надійності веб-сайтів і кращого розуміння IT-інфраструктури (апаратне забезпечення і мережеві зв’язки).

Нижченаведений перелік CAATTs містить кілька прикладів інструментів. Для кожного інструменту існують еквіваленти, які, ймовірно, не менш корисні.

Назва інструменту	Короткий опис
Аналіз безпеки Microsoft	Цей інструмент можна використовувати для оцінки рівня прогалин в операційних системах Microsoft та важливих налаштувань, пов’язаних з безпекою. Витрати: безкоштовно
Тестер SSL Labs	Цей інструмент допомагає оцінити якість зашифрованого

	зв’язку і написати детальний звіт. Витрати: безкоштовно
NMAP	Nmap (Мережевий сканер) – це сканер безпеки, за допомогою якого виявляють хости і сервіси в комп’ютерній мережі, створюючи таким чином «карту» мережі. Витрати: безкоштовно
OWASP ZAP	Zed проксі Attack (ZAP) – це легкий у використанні інтегрований інструмент для тестування проникання, який виявляє вразливі місця у веб-додатках. Витрати: безкоштовно
Splunk	Splunk збирає, індексує і заносить (у режимі реального часу) дані реєстру у сховище пошуку, з якого може генерувати графіки, звіти, попередження, панелі приладів та візуалізацій. Витрати: безкоштовно для особистого використання (500 мегабайт на день)
Flexicon Disco	DISCO – це інструмент процесу видобутку, який дозволяє аналізувати бізнес-процеси на основі реєстру подій. Головна ідея – видобувати знання з реєстру подій, записаного інформаційною системою. Витрати: на запит, однак можна завантажити безкоштовно
IDEA	IDEA® - це інструмент аналізу даних, призначений допомагати аудиторам швидко проводити аналіз даних, аби покращити аудити і виявити недоліки системи контролю. Важливими характеристиками є гарантія цілісності даних та забезпечення легкого аналізу понад 100 команд, пов’язаних з аудитом. Витрати: на запит
Qlikview	QlikView – це Платформа бізнес-інтелекту, яку аудитори також можуть використовувати для аналізу даних. Можна використовувати системи Планування ресурсів підприємства як джерело даних. Витрати: на запит, однак можна завантажити безкоштовно
BWISE	Це рішення для програмного забезпечення з корпоративного управління, ризиків та дотримання законодавства, яке аудитори можуть використовувати для аудиту програмного забезпечення Планування ресурсів підприємства, таких як SAP і Oracle EBS. Витрати: залежно від реалізації

Приклад використання інструментів IT-аудиту

З метою посилення системи внутрішнього контролю організації, керівництвом прийнято рішення щодо впровадження системи моніторингу - спеціального програмного продукту, який дозволяє здійснювати (он-лайн, тобто в режимі реального часу) контроль за станом проведення закупівель робіт, товарів та послуг за державні кошти.

Зазначений програмний продукт дозволяє фіксувати в автоматичному режимі та здійснювати контроль на етапах від формування річного плану закупівель, початку процедури закупівлі, процесу укладання договорів до фактичного постачання продукції (підтвердження факту виконання робіт, надання послуг), що сприяє оперативному прийняттю керівництвом організації рішень стосовно фінансового ресурсу.

Програмний продукт органічно інтегровано в систему бухгалтерського обліку

організації. В системі реалізовано надання регламентованого доступу до повноважень на здійснення операцій.

З метою оцінки системи внутрішнього контролю організації та її підрозділів, найбільш прийнятним у даному випадку буде проведення аудиту ефективності, в рамках якого доцільно використовувати інструменти IT-аудиту (змішаний аудит).

Тобто стан проведення закупівель доцільно провести звичайними методами основним складом аудиторської групи. Водночас, фахівець з IT-аудиту за допомогою набору інструментів IT-аудиту для конкретних завдань може значно поширити можливості аудиторської групи у визначенні найбільш ризикових сфер та наданні практичних рекомендацій.

Так, наприклад, використання інструменту Nmap дозволить спеціалісту з IT-аудиту виявити хости і сервіси в комп'ютерній мережі, створити карту мережі та надати керівництву організації рекомендації щодо посилення обмежень прав доступу до системи.

Використання інструменту OWASP ZAP, яким можливо провести у тому числі й тестування проникнення, та який дозволить виявити вразливі місця у веб-додатках, надає можливість рекомендувати керівництву організації ініціювати посилення захисту інформації в цілому, що вкрай важливо в системах, інтегрованих в систему управління фінансами організації з причин ризику фінансових втрат.

Використання інструменту Flexicon Disco дозволить проаналізувати бізнес-процеси на основі реєстру подій, які реєструються системою та надати рекомендації щодо корекції найбільш неефективно діючих процесів в ході проведення закупівель робіт, товарів та послуг.

5. Процес аудиту: етапи IT-аудиту

У цьому розділі коротко описуються основні кроки[13], які будь-який IT-аудитор повинен пройти, при проведенні IT-аудиту.

5.1. Кроки IT аудиту

1. Попереднє дослідження об'єкта аудиту та планування внутрішнього аудиту;

2. Проведення аудиту та аналіз;

3. Підготовка аудиторського звіту;

4. Відстеження результатів впровадження аудиторських рекомендацій.

Процес IT-аудиту в зазначених аспектах не відрізняється від будь-яких інших видів аудиту та здійснюється відповідно до тих самих кроків.

5.2. Попереднє дослідження об'єкта аудиту та планування внутрішнього аудиту

[13] детальний опис загального процесу міститься у Методологічних вказівках з внутрішнього аудиту для державного сектору України

Попереднє дослідження об'єкта та планування аудиту є першим етапом у процесі внутрішнього аудиту. Його метою є прийняття рішення щодо необхідності та фокусу дослідження, збір інформації про об'єкт аудиту, включаючи аналіз процесу та діючих в його межах системних контрольних заходів, визначення питань аудиту, методів і критеріїв, та складання програми аудиту.

Цей етап має наступну послідовність (кроки):

- постановка завдання;
- попереднє планування аудиторського дослідження;
- установча робоча зустріч з представниками об'єкта аудиту;
- підготовка програми аудиту.

Постановка завдання

На цьому кроці необхідно визначити:

- напрям аудиту та тему дослідження;
- мету аудиту та очікувані результати;
- об'єкт аудиту (за потреби пріоритетні фокуси в межах об'єкта);
- ключові питання аудиту та ризики;
- окремі ключові початкові обмеження (або межі) аудиту, наприклад, термін проведення дослідження та період, що буде охоплений аудитом;
- склад аудиторської групи (в ході попереднього дослідження в залежності від потреб склад групи може бути доповнений/відкоригований, але на цьому кроці в обов'язковому порядку має бути призначено керівника групи) та інші ресурси, необхідні для проведення дослідження (наприклад, обсяг необхідних для відрядження коштів).

Також на цьому кроці може бути підготовлений розпорядчий документ на проведення аудиторського дослідження.

Як правило, остаточне визначення переважної більшості зазначених аспектів перебуває у сфері повноважень/відповідальності керівництва установи.

Склад аудиторської групи формується виходячи із напряму внутрішнього аудиту, його теми та головних завдань. Досвід, навички та спеціалізація внутрішніх аудиторів мають відповідати особливостям, обсягам та рівню покладених на них завдань. За необхідності одержання додаткових знань та навиків у конкретній сфері до проведення внутрішнього аудиту можуть залучатися інші фахівці установи або залучені експерти.

Попереднє планування аудиторського дослідження

Цей крок передбачає попередній збір та аналіз інформації про об'єкт аудиту, яка стосується процесу, цілей, ризиків, заходів контролю, тощо, з

метою визначення усіх базових аспектів аудиту, які формують проект програми аудиту.

Наступним кроком дослідження є обговорення проекту програми внутрішнього аудиту (Плану аудиту) із представниками об'єкта аудиту в ході установчої зустрічі.

Попередній аналіз дозволяє збирати інформацію щодо об’єкта аудиту без необхідності її детальної перевірки. Метою збору та аналізу даних на цьому кроці є визначення базових аспектів аудиту, необхідних для розробки проекту програми аудиту. Для цього слід:

- описати основні процеси об’єкта аудиту (мета – їх глибоке розуміння);
- визначити основні ризики у досягненні операційних цілей;
- визначити та описати ключові системні заходи контролю;
- за результатами аналітичного контролю виділити сфери, що потребують детального контролю;
- отримати іншу інформацію, що характеризує базові аспекти аудиту, які включаються до проекту програми аудиту.

Базовими аспектами аудиту, що в подальшому формують основу програми аудиту, і підлягають визначенню на цьому кроці є:

- конкретизація цілей та уточнення об'єкта аудиту;
- визначення меж та обмежень аудиту;
- визначення основних питань аудиту та ризиків;
- визначення основних методів і процедур проведення дослідження;
- критерії аудиту, які будуть застосовуватися;
- встановлення послідовності та термінів виконання робіт (включаючи підготовку проекту аудиторського звіту);
- розподіл обов'язків в межах аудиторської групи.

Установча робоча зустріч із представниками об'єкта аудиту

Метою такої зустрічі є пояснення представникам об'єкта аудиту його базових аспектів, їх обговорення та за потреби уточнення. Під час такої зустрічі обговорюються як методологічні аспекти дослідження (цілі, питання, обсяги дослідження та документи, необхідні для його проведення), так і адміністративні (терміни основних етапів проведення, контакти посадових осіб, порядок отримання інформації та документів, тощо).

Підготовка програми аудиту

Заключним кроком етапу проведення попереднього дослідження та планування аудиту є остаточне формування та затвердження програми внутрішнього аудиту.

Відповідно до Національних стандартів внутрішнього аудиту, програма

внутрішнього аудиту визначає:

- напрям внутрішнього аудиту;
- цілі внутрішнього аудиту;
- підставу для проведення внутрішнього аудиту;
- період, що охоплюється внутрішнім аудитом;
- термін проведення внутрішнього аудиту;
- початкові обмеження щодо проведення внутрішнього аудиту (часові, географічні та інші);
- питання, що підлягають дослідженню з урахуванням оцінки ризиків (операції, ділянки бухгалтерського обліку та внутрішнього контролю установи, тощо);
- обсяг аудиторських прийомів і процедур за кожним фактором ризику;
- послідовність і терміни виконання робіт;
- склад аудиторської групи;
- планові трудові витрати.

Аудиторська група повинна визначати цілі аудиту шляхом відповіді на запитання: "чому ми проводимо аудит?" Як правило, цілі аудиту вказують на те, що керівник буде робити із результатами аудиту. Наприклад, "проведення IT-аудиту з метою розробки рекомендацій для вдосконалення існуючих заходів контролю".

Програма внутрішнього аудиту складається у письмовому вигляді, підписується керівником підрозділу внутрішнього аудиту та затверджується керівником установи до початку її виконання. Внесення змін до програми внутрішнього аудиту здійснюється в порядку її затвердження.

5.3 Проведення аудиту та аналіз

Методи і процедури проведення дослідження та подальшого аналізу зібраних даних **напряму залежать від типу аудиторського висновку**, який передбачений аудитом в залежності від його напряму, теми та цілей. Тому перед тим як обрати необхідні методи проведення аудиту потрібно визначитись з типом аудиторського висновку, який буде надано за результатами аудиту.

При здійсненні IT-аудиту **аудиторські висновки**, мають вигляд узагальненого формулювання підтверджених доказовою базою проблем аудиту (питань аудиту/гіпотез)[14]. Для підготовки висновку аудиторська група, як правило, також використовує критерії, які окремо визначаються для підтвердження/не підтвердження кожної проблеми.

[14] На відміну від *оціночного висновку*, який формулюється виключно за результатами фінансових аудитів та/або аудитів відповідності, і який за термінологією у міжнародній практиці прийнято називати ***аудиторською думкою.***

Підґрунтям для формування аудиторських висновків є **фактичні знахідки**, отримані в результаті аналізу аудиторських доказів, інформації зібраної в процесі аудиту під час документування різних питань аудиторського дослідження. В окремих випадках вони можуть бути єдиним результатом дослідження. Зокрема, це може бути у випадку, коли аудитору ставиться завдання оцінити чи існують певні проблеми або ризики у процесі (як наприклад, ймовірність помилки у процесі автоматизованої обробки інформації).

Зазвичай фактичні знахідки є частиною доказової бази аудиторського звіту та описуються в аналітичній частині звіту, а на їх основі формулюються аудиторські висновки.

При підготовці аудиторських висновків або пошуку фактичних знахідок, знадобиться більш широкий спектр методів збору доказової бази ніж для надання оціночного висновку.

Для формулювання аудиторського висновку та пошуку знахідок, доцільно проводити тестування, інтерв'ю, застосування опитувальника, аналіз документів тощо.

Визначення джерел та методів збору аудиторських доказів.

Методи, що реалізуються в ході аудиту, повинні бути визначені у програмі аудиту.

Збір аудиторських доказів є необхідним елементом аудиторського дослідження, який допомагає аудитору обґрунтувати думки та надати відповідні аудиторські висновки.

При проведенні IT-аудиту збір аудиторських доказів стосується ефективності, результативності, надійності та безпеки систем IT.

Під ***аудиторським доказом*** розуміється зібрана та задокументована надійна інформація, яку використовує аудитор для обґрунтування висновків за результатами внутрішнього аудиту.

Аудитори зобов'язані визначати точну, належну та необхідну для досягнення цілей інформацію. Зі свого боку, відповідальність за достовірність інформації та документації, наданої аудиторам, несуть посадові особи установи, що її склали, затвердили, підписали чи засвідчили.

Аудитори повинні зібрати, проаналізувати, оцінити і документально оформити інформацію в тих обсягах, що будуть достатніми для досягнення цілей/мети аудиторського дослідження, а також отримати таку кількість аудиторських доказів, яка б дала можливість зробити необхідні висновки, при використанні яких буде підготовлено аудиторський звіт.

Обрані методи аудиту, процедура їх застосування та обсяг вибірки повинні **забезпечувати обґрунтованість висновків** за результатами аудиторського дослідження об'єкта внутрішнього аудиту.

Як правило, усі ці аспекти визначаються аудиторською групою ще на етапі попереднього дослідження та зазначаються у програмі аудиту, однак в процесі проведення аудиту може виникати необхідність їх доповнення/коригування.

Аудиторські докази діляться на:

- **документальні докази**, що включають документи, звіти, нормативні акти, внутрішні регулюючі документи, реєстри, листи, контракти, інвойси, тощо;
- докази, отримані за результатами інтерв'ю;
- **аналітичні докази**, що включають виписки із рахунків, розрахунки, графіки та інші докази, отримані за результатами аналітичних процедур;
- **фізичні докази**, що включають спостереження, фотографію, тощо.

Методи та інструменти[15]:

- аналітичний контроль;
- тестування систем контролю;
- документальна перевірка;
- вибірка;
- фактична перевірка, обстеження, спостереження, перевірка на місці;
- опис процесів (побудова блок-схем);
- повна перевірка (відповідності) процесу;
- опитувальники /анкетування;
- інтерв'ю персоналу об'єкта аудиту / залучених третіх сторін;
- вивчення нормативно-правової бази, інших документів;
- спеціальна перевірка, експертна оцінка.

Джерела отримання інформації

- нормативно-правові акти, внутрішні інструкції об'єкта аудиту;
- положення про організацію, організаційна структура;
- проекти планів заходів, звітів, статистичних даних, протоколів;
- дані первинних документів і звітів, у яких відображена основна інформація про процеси та операції;
- звіти, документи, облікові регістри та інша інформація про транзакції / фінансові процеси;
- фінансова, бюджетна, статистична, податкова звітність;
- матеріали внутрішніх та зовнішніх контрольних заходів;

[15] Поряд із зазначеними інструментами під час ІТ-аудиту, при необхідності, застосовуються специфічні, притаманні цьому напрямку аудиту, інструменти (див. підрозділ 4.3 цього посібника).

- дані, отримані за результатами експертних перевірок;
- інші документи, матеріали та інформація.

Проведення аудиту повинно супроводжуватися постійними контактами між аудиторської групою та об'єктом аудиту, а також персоналом та керівництвом об'єкта аудиту. Неформальні обговорення є корисним інструментом отримання додаткової інформації про потенційні проблеми та слабкості системи.

Кількісний та якісний аналіз даних, формування доказової бази

Цей крок передбачає застосування аналітичних процедур, ефективне та дієве використання засобів для аналізу й оцінки інформації та зібраних в ході аудиту даних.

Оцінка – це результат порівняння зібраних даних (чи аудиторських доказів) відповідно до попередньо визначених критеріїв аудиту.

Якщо аналітичні процедури демонструють певні тенденції, ознаки невідповідності щодо окремих результатів/транзакцій, внутрішній аудитор додатково їх переглядає, поглиблено вивчає, а за необхідності проводить інтерв'ю з метою пошуку роз'яснень, причин невідповідності та забезпечення впевненості. Виявлені, але не пояснені в результаті аналітичних процедур зв'язки та неочікувані результати, можуть вказувати на важливі факти, такі як: можлива помилка, порушення або зловживання. Такі невизначеності, встановлені за результатами аудиту, повинні доводитися до керівника підрозділу внутрішнього аудиту, а за необхідності до керівництва установи.

Наступним кроком є **документування робочих матеріалів**, тобто одержаної в ході аудиту інформації та заходів і результатів аналізу, яка є основою доказової бази для аудиторських знахідок, висновків/оціночних висновків та рекомендацій.

Як правило, керівник аудиторської групи переглядає, аналізує та узагальнює робочі документи, підготовлені членами групи. Ці документи накопичуються та зберігаються в аудиторському файлі (матеріалах справи внутрішнього аудиту) та повинні:

- сприяти плануванню, проведенню та нагляду за проведенням аудиту;
- документально підтверджувати інформацію та факти, викладені в аудиторському звіті;
- документувати рівень досягнення цілей аудиту;
- складати основу для проведення щорічних оцінок якості та підготовки програм забезпечення та підвищення якості;
- містити докази на випадок скарг, розслідувань, контролю за

матеріалами аудиту;

- сприяти професійному розвитку внутрішніх аудиторів.

Обсяги документування та відповідно розмір і наповнення справ внутрішнього аудиту (аудиторських файлів) є різним та залежить від аудиту. Однак незалежний оцінщик, переглядаючи матеріали справи (за потреби), повинен відтворити увесь процес аудиту та знайти відповідні аудиторські документи, що підтверджують аудиторські знахідки, висновки та оціночні висновки.

Справи внутрішнього аудиту (аудиторські файли) повинні містити: робочу програму, план аудиту, аудиторський звіт, зібрані аудиторські докази (результати тестувань, документальних перевірок, копії первинних документів, аудиторські розрахунки, звіти за результатами інтерв'ю, результати опитувань, тощо) та спосіб аналізу даних, яким чином аудиторська група дійшла відповідного аудиторського висновку та рекомендації. Задокументована послідовність усіх етапів процесу аудиту носить назву "аудиторського сліду".

Останнім кроком на етапі проведення аудиту – є **заключна зустріч між аудиторською групою та керівництвом об'єкта аудиту**.

Мета цієї зустрічі – обговорити та узгодити попередні аудиторські знахідки та рекомендації. Така зустріч завжди є доцільним кроком, адже не залежно від рівня професіоналізму проведеного аудиту, можуть виникнути помилки та/або непорозуміння (неправильне/неоднозначне трактування) щодо фактів та аудиторських знахідок, що в підсумку вплине на формулювання аудиторських висновків і рекомендацій.

Попереднє представлення одержаних знахідок і рекомендацій керівництву об'єкта аудиту забезпечує додаткову впевненість, що знахідки базуються на достовірних фактах/інформації, а підготовлені рекомендації є реалістичними та доцільними. Залучення керівництва об'єкта аудиту до обговорення знахідок і попередніх рекомендацій також автоматично дає початок процесу їх розуміння та прийняття.

У ході підготовки до заключної зустрічі із об'єктом аудиту, аудиторська група проводить оцінку важливості знахідок. Заключна зустріч повинна зосереджуватися на найбільш вагомих аспектах. Результати заключної зустрічі заносяться у протокол, який зберігається в справі внутрішнього аудиту (аудиторському файлі), а тому є складовою частиною "аудиторського сліду".

Заключним результатом цього етапу дослідження є формулювання аудиторською групою проекту аудиторських висновків (знахідок) та рекомендацій.

При цьому слід пам'ятати, що рекомендації повинні надаватися якщо

існує потреба у вдосконаленні, а у процесі проведення аудиту зібрано достатню доказову базу, що підтверджує таку потребу. Ключові аудиторські знахідки, виявлені причини проблем та/або ризиків є основними принципами для розробки належних рекомендацій.

Як вже зазначалось за результатами проведення ІТ-аудиту складається відповідний висновок/висновки у вигляді узагальненого формулювання підтверджених доказовою базою проблем аудиту.

5.4. Звітування за результатами ІТ-аудиту

Аудиторський звіт є найбільш важливим результатом процесу аудиту, оскільки у ньому представлені аудиторські висновки (знахідки) та рекомендації, які забезпечують додаткову цінність від аудиту. Добре написаний і представлений керівництву аудиторський звіт сприяє розумінню необхідності змін (вдосконалення) та спонукає керівництво до вжиття відповідних коригуючих дій.

Аудиторський звіт переслідує три основні цілі:

- *інформувати керівництво установи щодо результатів аудиту та стану об'єкта аудиту;*
- *переконати керівництво установи, що аудиторські висновки (знахідки) та рекомендації дієві й важливі;*
- *переконати керівництво установи вжити відповідні дії.*

Так, звіт за результатами внутрішнього аудиту повинен відповідати наступним характеристикам:

точність – звіт повинен базуватися на точних і достовірних фактах;

чіткість – звіт повинен бути зрозумілим, чітким, не містити неоднозначних трактувань. Текст повинен бути доступним, а не потребувати додаткових коментарів та роз’яснень;

об’єктивність – знахідки та рекомендації повинні бути об’єктивними та якісно відображати важливі аспекти дослідження;

лаконічність – звіт повинен бути чітким, не переобтяженим зайвою інформацією, однак це не означає, що звіт повинен бути коротким;

правдивість – звіт повинен у дипломатичний спосіб представляти "чутливі для об’єкта аудиту" аспекти. Фокусуватися на подальших вдосконаленнях, а не на несуттєвій критиці людей чи попередніх подій;

своєчасність – звіт готується у визначені терміни;

мати коригуючий характер – звіт має містити посилання, зроблені на коригуючи дії проведені в ході (за результатами) аудиту. Така інформація завжди додає цінності аудиторському звіту.

Крім того:

- Звіт повинен базуватися та враховувати очікування читача.
- Структура звіту повинна бути чіткою та логічною.
- Звіт повинен бути написаний чіткою та зрозумілою мовою
- Звіт повинен бути збалансований та впливовий.
- Аудиторська група повинна розвивати знання та навики в частині підготовки аудиторських звітів.

Процес підготовки аудиторського звіту має низку послідовних дій, які представлено нижче.

1. Підготовка аудиторських висновків/знахідок.
2. Розробка аудиторських рекомендацій.
3. Підготовка проекту звіту – стандартний формат.
4. Перевірка керівником підрозділу внутрішнього аудиту.
5. Заключна зустріч із представниками об'єкта аудиту.
6. Підготовка остаточного аудиторського звіту.
7. Представлення результатів аудиту керівництву установи.
8. Представлення результатів аудиту іншим зацікавленим сторонам.
9. Підготовка Плану заходів впровадження рекомендацій[16].

5.5. Відстеження результатів впровадження аудиторських рекомендацій

Остаточним завершенням внутрішнього аудиту є етап відстеження результатів **впровадження аудиторських рекомендацій**.

Основи для успішного проведення цього етапу діяльності внутрішнього аудиту мають бути закладені при підготовці самих рекомендацій.

Для забезпечення можливості подальшого відстеження результатів їх впровадження, самі рекомендації повинні відповідати низці ключових правил, зокрема, вони мають:

- *містити конкретні, доцільні та економічні заходи (це означає, що кошти на проведення заходів не повинні перевищувати очікуваного ефекту);*
- *за кожним заходом визначати відповідальних виконавців і чіткі терміни виконання. Якщо реалізація одного заходу, передбачає декілька виконавців усі вони мають бути визначені, при чому для кожного з них доцільно встановити персональні терміни. В подальшому, у разі невиконання заходу, це дозволить чітко розмежувати сфери відповідальності та встановити хто із співвиконавців і на якому етапі не забезпечив його реалізації;*
- *бути орієнтовані на конкретний результат (містити очікуваний*

[16] за рішенням керівника установи.

результат їх впровадження), досягнення якого також має бути чітко визначено у часі;

- *за можливості визначати методи, періодичність та часові рамки процесу відстеження / моніторингу.*

Дотримання цих правил на етапі формування аудиторських рекомендацій суттєво поліпшує подальший процес відстеження результатів їх впровадження та дозволяє демонструвати "додаткову цінність" (реальний економічний ефект) від кожного проведеного внутрішнього аудиту.

Загалом відстеження результатів впровадження аудиторських рекомендацій забезпечує такі основні цілі:

- підвищує результативність аудиторських звітів;
- стимулює осіб, відповідальних за реалізацію визначених заходів, до практичного впровадження розроблених рекомендацій;
- оцінює діяльність аудиторської групи;
- стимулює ініціативу до навчання та розвитку, оскільки розроблення та практична реалізація заходів із відстеження впровадження рекомендацій сприяють підвищенню фахового рівня та набуттю практичного досвіду.

Процес відстеження результатів впровадження аудиторських рекомендацій повинен забезпечити відстеження управління високими ризиками та належний рівень впровадження розроблених заходів. Відповідно аудиторські рекомендацій мають бути пріоритезовані за рівнем важливості. Рекомендації високого рівня важливості повинні постійно відстежуватися, а результати відстеження доповідатися вищому керівництву.

У ході звітування за результатами відстеження впровадження аудиторських рекомендацій, особлива увага керівництва органу звертається на взаємозв’язок між аудиторськими знахідками та відповідними рекомендаціями.

Виділяють чотири рівні заходів відстеження аудиторських рекомендацій:

- *усне інформування* – найпростіший спосіб відстеження аудиторських рекомендацій, який передбачає регулярне спілкування із відповідальними за впровадження рекомендацій фахівцями об'єкта аудиту, спостереження, аналіз прогресу діяльності, тощо. Це може бути зроблено швидко, однак дає обмежені докази вжиття заходів;
- *документальне відстеження* – такий спосіб передбачає офіційне листування із відповідальними за впровадження рекомендацій фахівцями, направлення їм періодичних нагадувань, запитів, тощо; застосування форм (опитувальників) для одержання підтвердження від об’єкта аудиту про вжиті заходи. Письмова відповідь забезпечує більш якісні докази вжиття заходів, але все ще потребує незалежної перевірки внутрішніми аудиторами рівня впровадження рекомендацій;

• *фактичне відстеження* – передбачає короткі візити на об’єкт аудиту та прямий зв’язок внутрішніх аудиторів із об’єктом аудиту для збору доказів щодо заходів із впровадження рекомендацій;

• *послідуючий аудит* – проведення досліджень стану впровадження рекомендацій, наданих за результатами попередньо проведених аудитів.

Керівник підрозділу внутрішнього аудиту визначає які способи (чи їх поєднання) застосувати для відстеження результатів впровадження аудиторських рекомендацій в кожному окремому випадку.

Відстеження та моніторинг результатів впровадження аудиторських рекомендацій є частиною процесу управлінської підзвітності. Адже інформація, отримана за результатами відстеження результатів впровадження аудиторських рекомендацій, забезпечує регулярний, надійний та важливий внесок у процес управління ризиками в системі відповідного органу влади. Разом з іншими факторами така інформація формує основу для щорічної актуалізації ризиків у системі відповідного органу влади, на підставі яких у свою чергу формуються плани аудиторської діяльності.

Крім того, дотримання процесу моніторингу та відстеження впровадження рекомендацій виконує ще і стимулюючу роль, вимагаючи від осіб, відповідальних за реалізацію визначених заходів, конкретних дій та кроків, направлених на їх практичне впровадження. Якщо за результатами відстеження внутрішній аудитор вважає, що відповідальні за впровадження посадові особи об'єкта аудиту не проводять заходів, передбачених в рамках реалізації аудиторських рекомендацій, що має наслідком не зменшення (а можливо і збільшення) рівня ризиків, він повинен поінформувати про це керівника органу влади.

Результати впровадження аудиторських рекомендацій повинні системно відстежуватися, а реалізовані заходи повинні оцінюватися та постійно доповідатися керівництву органу влади. Лише такий підхід забезпечує та демонструє керівникові органу влади (установи) ефективність та результативність діяльності підрозділу внутрішнього аудиту.

6. Забезпечення якості в ІТ аудитах

Проводячи ІТ аудити, підрозділи внутрішнього аудиту повинні забезпечити дотримання Національних стандартів внутрішнього аудиту[17] та

[17] Стандарти внутрішнього аудиту, затверджені наказом Мінфіну від 04.10.2011 № 1247, та зареєстровані в Мін’юсті 20.10.2011 за № 1219/19957.

Кодексу етики[18]. Забезпечення якості – це процес відстеження цієї відповідності шляхом оцінки процесу аудиту на різних рівнях: постійний моніторинг процесу аудиту та періодична внутрішня та зовнішня оцінки якості. Більш детально процес гарантії якості для будь-якого виду аудиту описано у Главі 6 «Методологічних вказівок для внутрішнього аудиту в державному секторі». Однак, у даній частині коротко зазначено найбільш важливі аспекти забезпечення якості при проведенні ІТ аудиту.

Забезпечення якості діяльності служби внутрішнього аудиту розпочинається із самого аудиторського процесу. Тому, аудитори повинні мати достатні професійні навики, знання та компетенції у різних ІТ-сферах, достатні для проведення аудиту відповідно до регламентуючих документів. Керівник служби внутрішнього аудиту повинен забезпечити організацію необхідного розвитку спроможностей персоналу.

Організація забезпечення якості процесу аудиту може здійснюватися у кілька напрямків. У випадку проведення ІТ-аудиту командою, рекомендується призначити керівника групи, який відстежуватиме відповідність регулюючим документам протягом кожного етапу аудиту (планування, проведення аудиту, аналіз, звітування та відстеження).

На кожному етапі проведення ІТ-аудиту, аудитор подає необхідні документи керівнику аудиторської групи і / або керівнику підрозділу внутрішнього аудиту для контролю якості. У ході проведення контролю якості, керівник групи чи підрозділу зосереджують свою увагу на питаннях раціональності ІТ-аудиту, вибраній методології аудиту, практичних підходах, критеріях аудиту, інструментах, що застосовуються та реалістичності планування. Залежно від завдання, інколи доцільно проводити аналіз процесу відбору критеріїв аудиту.

Підбираючи аудиторську групу, керівник групи (або керівник підрозділу внутрішнього аудиту) повинен враховувати (та перевіряти) чи визначені аудитори зможуть забезпечити належну об’єктивність та незалежність щодо об’єкту аудиту. Якщо підрозділ внутрішнього аудиту невеликий, керівник підрозділу повинен виконувати роль керівника групи. У будь-якому випадку керівник підрозділу внутрішнього аудиту несе відповідальність (та є підзвітним) за забезпечення якості в ході проведення аудиту.

[18] Кодекс етики працівників підрозділу внутрішнього аудиту, затверджений наказом Мінфіну від 29.09.2011 №1217 та зареєстрований в Мін’юсті 17.10.2011 за № 1195/19933.

Додаток "IT-основи"

COBIT 5 (Завдання управління для інформаційних та суміжних технологій, версія 5)

COBIT 5 – це пакет стандартів і вказівок, розроблених ISACA[19], який можуть використовувати IT-аудитори завдяки його вичерпності та повноті. Він містить міжнародно визнані завдання управління для інформаційних технологій підприємств усіх рівнів. Недолік COBIT полягає у тому, що він охоплює дуже багато процесів і містить великий масив інформації і матриць. Як наслідок, це може розпорошити увагу та дезорієнтувати IT-аудитора.

У першу чергу COBIT 5 – це основа для корпоративного управління. Її розроблено, щоб допомагати підприємствам діставати оптимальну цінність від IT шляхом підтримки балансу між отриманням користі, оптимізацією рівнів ризиків та використанням ресурсів. З цією метою описуються процеси для корпоративного управління інформаційними технологіями підприємства. Ці процеси згруповані у чотирьох розділах:

1. Узгоджувати, планувати і організовувати (APO).
2. Будувати, набувати і впроваджувати (BAI).
3. Доставляти, обслуговувати і підтримувати (DSS).
4. Здійснювати моніторинг, аналіз та оцінку (MEA).

Залежно від об'єкта IT-аудиту IT-аудитор може вибирати застосовані процеси. Наприклад, якщо Управління змінами і Безпека становлять об'єкт IT-аудиту (або його частину), IT-аудитор може врахувати наступні процеси:

- BAI06, Управління змінами
- BAI07, Управління прийняттям змін та перехідним періодом
- AP013, Управління безпекою
- DSS05, Управління сервісами безпеки
- MEA03, Моніторинг, аналіз і оцінка дотримання зовнішніх вимог

Для кожного процесу формулюються пов'язані з IT цілі з відповідними показниками. На цій основі IT-аудитор може розробляти критерії аудиту. Найбільший інтерес для IT-аудитора становлять наступні процеси:

- APO09, Управління договорами на послуги
- APO11, Управління якістю
- APO12, Управління ризиком
- APO13, Управління безпекою
- BAI01, Управління програмами і проектами
- BAI04, Управління доступністю і спроможністю
- BAI06, Управління змінами

[19] Асоціація аудиту і контролю за інформаційними системами

- BAI07, Управління прийняттям змін та перехідним періодом
- DSS01, Управління транзакціями
- DSS02, Управління запитом на послуги та управління інцидентами
- DSS05, Управління послугами з безпеки
- DSS06, Управління заходами контролю за процесом
- MEA02, Моніторинг, аналіз і оцінка системи внутрішнього контролю
- MEA03, Моніторинг, аналіз і оцінка дотримання зовнішніх вимог

Залежно від IT-об'єкта можуть застосовуватися також інші процеси.

COBIT 5 також доступний російською мовою на веб-сайті ISACA: http://www.isaca.org/COBIT/Pages/COBIT-5-russian.aspx

Приклад

За результатами проведеного аудиторського дослідження управлінських рішень посадових осіб, відповідальних за хід виконання однієї з дослідно-конструкторських робіт з розробки системи автоматизованого управління ресурсами для потреб Замовника.

В ході внутрішнього аудиту, після проведення перевірки щодо взяття на бухгалтерський облік у кількісному та вартісному виразі науково-технічних і матеріальних цінностей та результатів інтелектуальної діяльності, що були створені або придбані, перед аудитором виник ряд додаткових завдань, щодо вирішення питання перевірки потенційних ризиків, наявності та, за потребою, функціональності програмно-технічного засобу, який розроблявся.

Для вирішення зазначених завдань, інструментів, якими користуються аудитори недостатньо, тому було прийняте рішення експериментально використати для перевірки якості інформаційної системи та прикладних програм методологію, яку пропонує комплексний підхід COBIT та її ключову складову - модель оцінки процесів (COBIT Process Assessment Model, PAM) «**Придбання та впровадження**»:

AI 2. Придбання та підтримка програмних додатків;
AI 3. Придбання та обслуговування технічної інфраструктури;
AI 4. Забезпечення виконання операцій;
AI 5. Поставки IT ресурсів;
AI 6. Управління внесенням змін;
AI 7. Впровадження та приймання рішень і змін;
та «**Експлуатація та супровід**»:
DS 1. Визначення та управління рівнем обслуговування;
DS 2. Управління послугами сторонніх організацій;
DS 3. Управління продуктивністю і потужностями;
DS 4. Забезпечення безперервності IT сервісів;
DS 6. Визначення та розподіл витрат;
DS 10. Управління проблемами;
DS 11. Управління даними;
DS 13. Управління операціями по експлуатації систем.

Практично, дослідженням наданих на розгляд актів попередніх випробувань

комплексів засобів автоматизації дослідного зразка встановлено, що прийомна комісія провела попередні випробування вищевказаних засобів автоматизації відповідно до Програми і Методики випробувань: комплектність, працездатність; відповідність характеристик засобів автоматизації вимогам та можливість приймання засобів автоматизації в дослідну експлуатацію.

Зафіксовані результати випробувань свідчать про комплектність засобів автоматизації, крім того комісією документально зазначено, що до засобів автоматизації входять функціональні, технологічні підсистеми та комплекс технічних засобів, що забезпечують реалізацію функцій засобів автоматизації згідно їх призначення. Типові програмно-технічні комплекси, що реалізують функції підсистем, в наявності. Комісія пропонувала прийняти засоби автоматизації в дослідну експлуатацію. Вивченням документації на засоби автоматизації встановлено, що окремим пунктом зазначено склад засобів автоматизації, який складається з комплексу технічних заходів та комплексу програмних заходів.

Проте, аудитом встановлено, що у відповідних графах документації стосовно наявності спеціального програмного забезпечення є посилання на формуляри програмних комплексів, які входять до складу засобів автоматизації. У свою чергу документація не містить відомості щодо спеціального програмного забезпечення (зокрема, комплект ліцензійного ПЗ, програмне забезпечення геолокаційної підсистеми та інші).

Включення до складу засобів автоматизації програмного забезпечення не підтверджується наданими на вивчення відомостями машинних носіїв інформації комплексу засобів автоматизації.

У той же час, керівництвом було затверджено акт про завершення корегування робочої конструкторської документації дослідного зразка.

Дослідженням плану створення засобів автоматизації встановлено, що метою етапу було створення та впровадження окремих компонентів управління.

Відповідно до відомостей, зазначених у Акті приймання етапу та робочої документації, результатів випробувань дослідного зразка (визначення можливості приймання елементів засобів автоматизації в дослідну експлуатацію (у тому числі підсистем відображення інформації, управління функціонуванням, електронного документообігу, інформаційно-довідкової, електронної пошти, телекомунікаційної мережі та ін.)) аудитор дійшов до висновку, що:

- загальна характеристика засобів автоматизації дозволяє розробнику підготувати документацію для виготовлення дослідного зразка;
- обладнання, загальне та спеціальне програмне забезпечення засобів автоматизації об’єктів автоматизації передано Замовнику згідно з актами;
- роботи з розгортання, пусконалагодження та здавання в експлуатацію п’яти елементів дослідного зразка засобів автоматизації не виконані, хоча підтверджені актами приймання обладнання та виконання пусконалагоджувальних робіт;
- рішення, реалізовані програмним забезпеченням не достатні для організації функціонування засобів автоматизації;
- сукупність виробничих операцій створення засобів автоматизації потребують уточнення документації в частині технології монтажу обладнання та інсталяції програмних застосувань.

Враховуючи аудиторські знахідки аудитор прийшов до висновку, що створені в ході дослідно-конструкторської роботи засоби автоматизації не є системним рішенням (програмно-технічним комплексом), яке складається з технічних засобів та встановленим на ньому програмним забезпеченням.

Крім того, під час аудиту встановлено, що система внутрішнього контролю за виконанням дослідно-конструкторської роботи не забезпечила належної ефективності та

дієвості контролю за організацією обліку, збереження, економного та ефективного використання державних коштів.

Таким чином, станом на момент проведення аудиту документально встановлено зняття з обліку програмного забезпечення та інших об’єктів інтелектуальної власності, прийнятих й оплачених Замовником, що призвело до нанесення державі збитків через втрату активів при невиконанні у повному обсязі робіт дослідно-конструкторської роботи на загальну суму 18 391 997,85 гривень.

ITIL V3 (Бібліотека інфраструктури інформаційних технологій,[20] версія 3)

ITIL – це найкращий опис міжнародних практик з державного та приватного секторів. Ідеться про надання IT-послуг компанії, документування процесів, функцій та ролей Управління IT-службою (ITSM).

Головний наголос ITIL зроблено на IT-інфраструктуру. Типовий стандарт IT-інфраструктури складається з наступних компонентів:

- Комп’ютерне апаратне забезпечення: сервери, комп’ютери, центри даних, мережеві комутатори, центральні станції і роутери, тощо.
- Програмне забезпечення: управління програмним забезпеченням, яке вже готове і використовується персоналом. Розробка і обслуговування програмного забезпечення не входить до ITIL.
- Мережа: забезпечення мережі, зв'язок з Інтернетом, брандмауер і безпека.
- Людські ресурси, такі як мережеві адміністратори, розробники, дизайнери і загальні кінцеві користувачі з доступом до будь-якого пристрою або послуги IT. Це також частина IT-інфраструктури, особливо з початком розробки IT-послуг, орієнтованих на користувача.

Найкращі практики ITIL на даний час деталізовані у п’яти ключових публікаціях:

- Розробка стратегії
- Створення послуг
- Підготовка послуг до операційної діяльності*
- Операційна діяльність*
- Неперервне покращення послуг

*Залежно від об’єкту IT-аудиту, *Підготовка послуг до операційної діяльності* та *Операційна діяльність* будуть, ймовірно, найбільш корисними для IT-аудитора. Вони включають такі важливі процеси як Управління змінами, Управління доступом, Управління інцидентами та Управління прикладною програмою.

З належним знанням процесів ITIL аудитор зможе визначити правильні критерії аудиту, застосовані до об’єкта IT-аудиту, пов’язаного з IT-

[20] Називається бібліотекою, бо концепції і практики видані серією книг

інфраструктурою.

Prince2 (проекти в контрольованому середовищі. Версія 2)

Prince 2 – це методологія управління проектом, яка охоплює управління якістю, контроль і організацію проекту послідовно і узгоджено з цілями. Prince 2 використовується для IT-проектів, а також для багатьох інших видів проектів.

Ключові характеристики Prince 2 такі:

- Зосередження на виправданні бізнесу. Це означає, що проекти повинні узгоджуватися з бізнес-цілями організації-клієнта. Це принцип запобігає тому, щоб організації починали або продовжували проекти, які не можуть бути затвердженими в рамках корпоративної стратегії.
- Визначена організаційна структура для групи управління проектом. Ролі та обов'язки визначені і затверджені.
- Підхід до планування на основі продукту. За цим підходом усі результати проекту і його компонентів вважаються продуктами. Якщо проект полягає у запровадженні нової інформаційної системи, то кінцевим продуктом буде «робоча інформаційна система».
- Наголос на розділі проекту на етапи, якими можна управляти і які можна контролювати.
- Гнучкість у проекті, яку можна застосувати на відповідному рівні.

IT-аудитор може використовувати ці ключові характеристики, а також інші характеристики Prince2 для визначення критеріїв аудиту.

Проведення аудиту – це основа для моніторингу успіху будь-якого проекту. Аудит проекту важливий, щоб підтвердити, чи проект здійснений для цього бізнесу, перевірити, чи проект може перейти на наступний етап і також перевірити будь-які спеціальні питання, які виникають під час реалізації проекту. Найважливіше те, що аудити допомагають заспокоїти керівництво.

Користь від аудиту проекту може бути наступною:

- Найперше і найважливіше – здатність заздалегідь виявляти проблеми;
- Доступ до взаємозв'язків між результатами виконання, витратами проекту та часовими рамками проекту;
- Підвищення загальної продуктивності проекту;
- Здатність виявляти потенційні можливості;
- Скорочення витрат часу, зусиль, матеріалів та коштів.

Приклад

За результатами проведеного аудиторського дослідження управлінських рішень посадових осіб, відповідальних за процедуру закупівлі системи управління адміністративними процесами (далі – СУАП, Проект) та дотримання вимог чинного законодавства, встановленого порядку організації та, відповідно до вимог нормативних документів, технічної документації, умов контрактів (договорів) для потреб Замовника.

Довідково: У зв'язку зі складністю та великими обсягами функціональних процесів (дев'ять) адміністративно-господарської діяльності організації, які потребували автоматизації його управління, було заплановано реалізувати проект створення СУАП протягом чотирьох років у чотири черги.

Керівництво Проектом було покладено на заступника керівника організації.

Для безпосередньої розробки та впровадження системи була створена проектна група, до складу якої увійшли фахівці з інформаційних технологій, фахівці методологічної підтримки окремих адміністративно-господарських процесів (за напрямками), фахівці із захисту інформації тощо.

Організаційно-розпорядчі функції керівник Проекту здійснював через Управління інформаційних технологій. Начальник зазначеного управління був призначений заступником керівника Проекту та керівником проектної групи.

Підготовка до проведення внутрішнього аудиту та фактична перевірка в ході аудиту даних бухгалтерського обліку, наявності науково-технічних і матеріальних цінностей, результатів інтелектуальної діяльності, що були придбані, розкрили перед аудиторською групою ряд питань, потребуючих дослідження процесів управління проектами та, відповідно необхідності залучення фахівця, який має ряд спеціальних знань із зазначених питань.

В ході проведення внутрішнього аудиту, керівником підрозділу внутрішнього аудиту (за ініціативою керівника аудиторської групи) було прийняте рішення про додаткове залучення фахівця підрозділу внутрішнього аудиту, який (за дорученням керівника) проводив експериментальні дослідження практичного застосування передових практик з IT-аудиту.

Для вирішення зазначених завдань, аудитором було прийняте рішення використати методологію правління проектами «Prince 2».

В ході аудиту аудитором фокусувався акцент на взаємовідносинах Замовника, Виконавця та Користувачів.

Вищезазначений процес закупівлі програмного продукту було вивчено за вхідними та вихідними даними, специфічними цілями та діями, які було застосовано до кожного етапу закупівлі та впровадження.

Аудит здійснювався з використанням вивчення чотирьох процесів вищого рівня:

- DP – directing a project;
- SU – starting up a project;
- CS – controlling a stage;
- MP – managing stage boundaries.

Під час перевірки також використовувалась методологія щодо визначення організаційної структури управління проектом та поділу проекту на стадії управління та контролю.

Дослідженням встановлено, що з причин непрофесійних управлінських процесів в

організації, відсутності контролю за станом продукту на рівні CS (controlling a stage), ризик не впровадження закупленого за державні кошти програмного продукту привів до практичної його втрати.

Так, в ході аудиту встановлено, що для забезпечення реалізації Проекту організацією укладений договір щодо закупівлі дослідно-конструкторської роботи з 1 черги Проекту, загальною вартістю 25,03 млн. гривень, яку в подальшому було зменшено до 24,99 млн. гривень. Причини зменшення обсягів фінансування посадові особи обґрунтовано пояснити не змогли.

Роботи з розробки та втілення 1 черги Проекту проводилися протягом двох років. Кошти були використані на 100%.

Наприкінці першої черги втілення проекту повноваження щодо фінансового забезпечення та ведення обліку незавершеного виробництва і продукції в рамках виконання ДКР було передано до іншого підрозділу організації.

Опрацюванням та порівнянням наданої для дослідження інформації, аудитором було встановлено, що Сторонами неодноразово змінювалися умови договору (12 додаткових угод) щодо строків і обсягів проведення робіт і сум авансування та оплати робіт за етапами. Крім того, не зважаючи на проведене (без підтвердження законності витрачання авансу) авансування робіт безпідставно зменшувалася сума вартості спеціального обладнання, ліцензійного програмного забезпечення, закупленого в інтересах Замовника, та збільшувалася частка Виконавця робіт через залучення нових співвиконавців.

Далі був укладений договір щодо закупівлі ДКР з другої черги Проекту, загальною вартістю 12,15 млн. гривень. Протягом року проведено авансування та оплату робіт за договором у сумі 10,51 млн. грн., що складає 85% від суми договору. Через відсутність фінансування та договірних зобов'язань Сторін, роботи по цій ДКР у наступному не проводилися. Передбачені, в межах зазначеної ДКР, роботи, не проведені.

Паралельно з зазначеним договором також заключено ще п'ять договорів з іншими Виконавцями з метою забезпечення СУАП системою захисту інформації різних рівнів на суму близько 10 млн. гривень.

Аудитом встановлено, що рішення про необхідність проведення фінансових розрахунків, авансування та оплату ДКР приймалися керівництвом організації, про що видавалися розпорядження через відповідні відділи та управління головним виконавцям кошторисних підпрограм.

У той же час, на підставі наказу керівника організації, повноваження керівника Проекту від першого заступника були передані іншому заступнику. Після відсторонення останнього від посади, функції Замовника були надані начальнику Управління інформаційних технологій, який на підставі рішення керівника організації виконував функції замовника протягом двох років. При цьому, Керівник Проекту не був призначений.

Крім того, під час зміни керівництва не було проведено інвентаризацію продукції, придбаної в межах ДКР.

Аудиторським дослідженням встановлено, що втілена керівником Проекту заступником керівника організації, начальником управління інформаційних технологій, посадовими особами інших структурних підрозділів, у виконання І етапу ДКР практика щодо збільшення термінів виконання робіт за окремими етапами, при одночасному зменшені обсягів і вартості проавансованих з бюджету організації робіт[21], в подальшому була застосована під час збільшення кількості робочих етапів та інших дослідно-конструкторських робіт в рамках Проекту.

Вищевказані порушення щодо забезпечення посадовими особами організації виконання Проекту призвели до того, що жодна з робіт Проекту, незважаючи на

[21] з метою уникнення штрафних санкцій, перенесення на наступні етапи обсягів і вартості невиконаних за окремими етапами робіт для забезпечення їх *(наступних етапів)* попередньої оплати (авансування)

авансування робіт, фактично завершена не була.

Тобто проведена у повному обсязі (100%) оплата робіт за першим договором фактично не призвела до створення та впровадження І черги СУАП. При тому, аудитором встановлено, що через відсутність системи захисту інформації в СУАП подальше її прийняття в постійну експлуатацію неможливе.

У порушення встановленого порядку виконання дослідно-конструкторських робіт, етапів у їх межах, щодо послідовного використання в наступних роботах Проекту (нарощування досягнень), відповідальними посадовими особами було організоване паралельне виконання декількох робіт проекту, декількох етапів у межах одної роботи. Вищевказані дії спричинили неефективне використання бюджетних коштів.

Разом з тим, згідно з проведеним аналізом з'ясовано, що на об'єктах пілотної зони у окремих відділах та управліннях дослідна експлуатація не проводилася. Причинами не проведення дослідної експлуатації було зазначено: не підключення їх автоматичних систем до загально-інформаційної мережі організації, проведення реорганізаційних заходів; зміна місць дислокації тощо.

Жодним нормативним документом організації об'єкти І черги Проекту, з відповідним розподілом на функціональні підсистеми, визначені не були, їх обладнання комп'ютерною технікою не визначалося, підключення до загально-інформаційної мережі забезпечене та проведене не було.

В результаті виконання робіт створювався дослідний зразок І черги СУАП, в якому підлягали автоматизації робочі місця лише на Центрі комутації і на 25 визначених об'єктах органів управління організацією всіх рангів. Об'єднанням на них засобів автоматизації в єдині комплекси, на основі структурованих кабельних мереж, було передбачено створити локальні комп'ютерні мережі і відповідні автоматизовані технологічні комплекси. Об'єднанням останніх, на базі існуючої корпоративної комп'ютерної мережі організації, передбачалося створити разом з Центром комутації – дослідний зразок І черги за п'ятьма визначеними функціональними напрямками. Крім того, на Центрі впроваджень для забезпечення системи розробки, системи якості, вивчення технологічних процесів у дослідному зразку, їх аналізу, опрацювання, коригування, налагодження та запровадження на об'єктах дослідного зразка І черги СУАП була створена автоматизована система еталонних моделей.

Під час аудиту встановлено, що при виконанні покладених на них організаційно-розпорядчих функцій, в ході виконання Проекту та його супроводження, у порушення встановленого в організації порядку забезпечення комп'ютерною технікою та норм передбачених технічними завданнями на виконання робіт, за розподілом розробленим начальником управління інформаційних технологій та затвердженим заступником директора фактично було організовано та проведено наднормативне забезпечення структурних підрозділів 86 комплектами ПЕОМ, що спричинило зайве та неефективне витрачання коштів бюджету на суму 774 тис. гривень.

Вибірковою перевіркою законності використання в зазначених підрозділах виданого у межах виконання Проекту, майна встановлено, що воно не завжди використовувалося за призначенням.

Таким чином, аудитором за результатами проведеного за допомогою методології управління проектами «Prince 2» зроблено висновок, що повнота і достовірність даних обліку щодо створеного, поставленого та оплаченого за кошти державного бюджету продукту, обладнання, монтажних і пусконалагоджувальних робіт в рамках Проекту відповідальними посадовими особами не забезпечені. З причин низки неефективних управлінських рішень, відсутності контролю за процесом створення СУАП система управління адміністративними процесами в організації не впроваджена.

ASL (бібліотека послуг прикладних програм)

ASL – це опис найкращих практик, які використовуються для стандартизації процесів в Управлінні прикладними програмами, основа для створення і обслуговування інформаційних систем і прикладних програм. ASL – суспільне надбання. Стандартизований підхід ASL сприяє професіоналізації IT-організації та більш ефективному способу роботи, оптимізації витрат і кращому розумінню та комунікації між залученими сторонами.

ASL має на меті професіоналізацію управління прикладними програмами. Він узгоджується з ITIL та BiSL. Деякі процеси ITIL, ASL і BiSL більш-менш однакові, наприклад, на управлінському рівні. Додану цінність ASL IT-аудитор може знайти з окремих питань управління прикладними програмами такими як дизайн, розробка, тестування і запровадження (нових) прикладних програм.

ASL складається з 6 груп процесів (a, b, c…), до яких входить 26 процесів на трьох рівнях:

1. Операційний рівень:
a. Підтримка прикладної програми (4 процеси)
b. Процеси зв'язку (2)
c. Обслуговування і оновлення прикладної програми (5)

2. Управлінський рівень:
a. Процеси управління (5)

3. Стратегічний рівень:
a. Стратегія прикладних програм (5)
b. Стратегія організації управління прикладними програмами (5)

IT-аудитор може використовувати цю основу для визначення критеріїв аудиту організацій, які розробляють і обслуговують прикладні програми. Найкраще підходять для застосування процеси на операційному та управлінському рівні.

BiSL (бібліотека послуг бізнес-інформації)

BiSL – це основа, яка описує стандарт для процесів у рамках управління бізнес-інформацією на стратегічному, управлінському та операційному рівні. BiSL – це суспільне надбання. BiSL описує процеси та заходи з точки зору клієнта надання інформації. Бізнес та клієнт (у цьому випадку) також називаються «організація користувача»: організація, яка використовує та визначає попит на IT.

BiSL зосереджується на тому, як бізнес-організації можуть покращити

контроль за інформаційними системами: попит на бізнес-підтримку, використання інформаційних систем, договорів та інших домовленостей з IT-постачальниками. BiSL пропонує супровід в управлінні бізнес-інформацією: підтримку у використанні інформаційних систем у бізнес-процесах, операційний IT-контроль та управління інформацією.

Бібліотека складається з рамкової основи, найкращих практик, стандартних шаблонів та самооцінки. У рамковій основі BiSL наведено опис усіх процесів, які роблять можливим контроль за інформаційними системами з точки зору бізнесу.

BiSL складається з 7 груп процесів (a, b, c…), до яких входить 23 процеси на трьох рівнях:

1. Операційний рівень:
a. Управління користуванням (3)
b. Управління функціональністю (4)
c. Зв'язок процесів на операційному рівні (2)

2. Управлінський рівень:
a. Процеси управління (4)

3. Стратегічний рівень:
a. Інформаційна стратегія (4)
b. Стратегія IT-організації (5)
c. Зв'язок процесів на стратегічному рівні (1)

IT-аудитор може використовувати цю основу для визначення критеріїв аудиту організацій користувача. У більшості випадків це буде функціональне управління. Найкраще підходять для застосування процеси на операційному та управлінському рівні.

ISO/IEC[22] 27001 і 27002

Міжнародна рамкова основа/стандарт безпеки ISO 27001 містить вимоги до управління інформаційною безпекою та до системи управління інформаційною безпекою (ISMS). ISO 27002 містить рекомендації з управління інформаційною безпекою на основі найкращих практик.

ISMS – це "системний підхід до створення, запровадження, функціонування, моніторингу, огляду, обслуговування та покращення інформаційної безпеки організації для досягнення бізнес-цілей". Він охоплює персонал, процеси і технологію, визнаючи, що інформаційна безпека це не тільки антивірусне програмне забезпечення, запровадження останньої версії брандмауера або блокування лептопів або вебсерверів. Загальний підхід до

[22] Міжнародна організація стандартизації International Organization for Standardization/ International Electrotechnical Commission. Usually the standard is called ISO 27001.

інформаційної безпеки має бути стратегічним, а також операційним. Слід визначити пріоритетність різних ініціатив з безпеки, інтегрувати їх та зробити між ними перехресні посилання, щоб забезпечити загальну результативність. ISMS допомагає організації узгоджено, послідовно та з мінімальними затратами координувати усі зусилля безпеки (як електронні, так і фізичні).

На даний час актуальною є версія 2014 року. ISO 27001:2014 чітко вказує, що заходи контролю не слід вибирати із наведеного у стандарті списку, а визначати їх шляхом опрацювання ризиків.

Для відбору застосованих заходів контролю головне провести вичерпну оцінку ризиків інформаційної безпеки організації на основі належної методології. Це означає, що керівництво організації відповідає за визначення ризиків, пов'язаних з втратою конфіденційності, цілісності і доступності інформації. Також потрібні аналіз та оцінка ризиків інформаційної безпеки, у тому числі визначення вірогідності того, що ризик матиме місце, а також рівнів потенційного ризику (його впливу).

При використанні цих стандартів для IT-аудитора важливо розуміти, що вони зосереджуються здебільшого на управлінській частині інформаційної безпеки. Хоча це важлива частина, вона не містить усіх можливих заходів контролю, які має реалізовувати організація. Наприклад, якщо організація використовує програмне забезпечення, яке має вихід в Інтернет, то заходи контролю з безпеки мають захищати IT організації від атак з Інтернету. ISO 27001 і 27002 містять тільки незначні заходи контролю в цій сфері. У цьому випадку слід враховувати напр. ISO 27032 — Керівництво з кібербезпеки (або іншу схожу основу).

Керівництво з аудиту інформаційних глобальних технологій 8 (GTAG 8)

Це керівництво з аудиту розроблене IBA для аудиту заходів контролю за прикладними програмами. Воно містить хорошу теоретичну базову інформацію. Заходи контролю за прикладними програмами – це ті заходи контролю, які належать до обсягу індивідуальних бізнес-процесів або прикладних систем, у тому числі редагування даних, розподіл бізнес функцій, баланс обробки підсумків, реєстрація транзакцій та звітування про помилки. Отже, ціль заходів контролю за прикладними програмами полягає у забезпеченні того, щоб:

- введення даних було точним, вичерпним, авторизованим і правильним;
- дані оброблялись належним чином у прийнятний часовий проміжок;
- збережені дані були точними і вичерпними;
- видані дані були точними і вичерпними;

- записувався процес проходження даних від вводу до зберігання, і до можливої видачі.

Найбільш важливі заходи контролю за прикладними програмами такі:

- Заходи контролю щодо вводу – використовуються здебільшого для перевірки цілісності даних, які вводяться в прикладну бізнес-програму, як введені безпосередньо персоналом, так і віддалено бізнес-партнером, або через веб-інтерфейс, або прикладну програму з Інтернет-доступом. Введення даних перевіряється, щоб забезпечити його відповідність визначеним параметрам.
- Заходи контролю щодо обробки – забезпечують автоматизованим засобом гарантії вичерпної, точної і авторизованої обробки даних.
- Заходи контролю щодо видачі даних – охоплюють результат обробки даних, мають порівнювати результати виданих даних із запланованим результатом, перевіряючи видані дані із введеними даними.
- Заходи контролю щодо цілісності – здійснюють моніторинг даних, які обробляються і зберігаються для забезпечення їхньої узгодженості та правильності.
- Управлінський слід – обробка історії заходів контролю, часто називається аудиторським слідом, яка дає керівництву можливість визначати транзакції та події, які записуються, шляхом відстеження транзакцій від джерела до видачі даних та у зворотному порядку. Ці заходи контролю також здійснюють моніторинг результативності інших заходів контролю та виявляють помилки якнайближче до джерел їх виникнення.

Заходи контролю за прикладними програмами використовуються замість ручних заходів контролю завдяки їх надійності. Якщо у прикладній програмі не застосовуються заходи контролю взагалі або застосовуються в обмеженому обсязі, ІТ-аудитору слід порекомендувати заходи контролю (за необхідністю – додаткові) за прикладними програмами з огляду на їх надійність. Після запровадження заходу контролю за прикладною програмою, якщо внесено мало змін у прикладну програму, базу даних або технологію, організація може покладатися на цей захід контролю до внесення суттєвих змін.

GTAG 8 може використовуватися ІТ-аудитором для аудиту цих заходів контролю за прикладними програмами. Ця основа містить поширені заходи контролю, пропоновані тести і перехресні посилання COSO.

Загальна програма аудиту/гарантії прикладних програм

Ця програма аудиту/гарантії розроблена ISACA, щоб допомогти ІТ-аудитору в розробці та проведенні огляду прикладної програми. Вона описує усі необхідні кроки, і ІТ-аудитор зобов'язаний змінювати цей документ, аби відобразити конкретне середовище, яке розглядається. Аудиторська група має узгодити Загальну програму аудиту/гарантії прикладних програм із бізнес-середовищем.

Конкретний огляд прикладної програми забезпечує ІТ-аудитора оцінкою

дизайну і результативності заходів внутрішнього контролю, операційної ефективності і результативності існуючої прикладної програми.

ІТ-аудитора-новачка найбільше може зацікавити ця Загальна програма аудиту прикладних програм, бо вона надзвичайно деталізовано визначає усі необхідні кроки для проведення огляду прикладної програми. Починається вона із "планування та визначення обсягу аудиту" та "планування аудиту прикладної програми". Усі кроки чітко розділені на менші кроки та конкретні тести. Наприклад:

6. ОБРОБКА ЦІЛІСНОСТІ І ЧИННОСТІ*
6.1 Цілісність і чинність даних Ціль аудиту/гарантії: цілісність і чинність даних має підтримуватися протягом циклу обробки, а виявлення транзакцій з помилками не має порушувати оброку чинних транзакцій.
6.1.1 Авторизація транзакцій Захід контролю: Визначено і запроваджено механізми для авторизації ініціювання і обробки транзакції, введено правило, що використовуються тільки належні та авторизовані прикладні програми та інструменти
6.1.1.1 Запитати і підтвердити, що транзакції опрацьовуються тільки після належної авторизації
6.1.1.2 Для вибраної прикладної програми запитати і підтвердити, що запроваджено розподіл обов’язків. Перевірити чи розподіл обов’язків запроваджено для вводу, зміни і схвалення даних транзакцій, а також чи запроваджено правила для підтвердження чинності

* Пояснення: 6.1 містить ціль аудиту, 6.1.1 містить захід контролю, який очікується в організації, а 6.1.1.1 і 6.1.1.2 – це ті дії ІТ-аудитора, завдяки яким він може визначити, чи є результативними заходи контролю.

При цьому Програма аудиту містить загально прийняті та застосовані кращі практики, а також перехресні посилання з COBIT 4.1 і COSO.