GUID 5100

Керівництво з аудиту інформаційних систем

INTOSAI

Керівництво INTOSAI випущені Міжнародною організацією вищих органів аудиту (INTOSAI) у складі Концептуальної основи стандартів INTOSAI. Додаткову інформацію можна знайти на сайті www.issai.org

INTOSAI

1) Схвалено як ISSAI 5100 — Керівництво з IT-аудиту у 2016 році.
2) Переглянуто та перейменовано на GUID 5100 «Керівництво з аудиту інформаційних систем» у 2019 році.

ЗМІСТ

1

ВСУП

1.1 GUID 5100 визначає загальну концептуальну основу для здійснення аудиту інформаційних систем у межах Концептуальної основи стандартів INTOSAI (IFPP). Це Керівництво GUID має на меті закласти підвалини для розроблення майбутніх GUID серії 5100–5109 для предметної області аудиту інформаційних систем у межах IFPP.

1.2 Концептуальна основа, подана в цьому GUID, узгоджена з *Фундаментальними принципами аудиту державного сектору* (ISSAI 100), *Фундаментальними принципами фінансового аудиту* (ISSAI 200), *Принципами аудиту діяльності* (ISSAI 300) та *Принципами аудиту відповідності* (ISSAI 400).

1.3 Вищі органи аудиту (ВОА) уповноважені перевіряти уряди та їхні установи відповідно до своїх повноважень.[1] Своєю діяльністю ВОА прагнуть сприяти ефективності, підзвітності, результативності та прозорості публічного (державного) управління.[2]

1.4 Уряди та інші суб'єкти публічного (державного) сектору постійно впроваджували інновації в інформаційних технологіях (ІТ) у свої інформаційні системи, щоб підвищити ефективність і результативність свого функціонування та надання різноманітних публічних (державних) послуг. Причина цього — те, що ІТ уможливили фіксацію, зберігання, оброблення, відтворення та доставлення інформації в електронному вигляді, що, у свою чергу, створює значні можливості для підвищення точності, конфіденційності та своєчасності показників інформаційних систем. Крім того, відбувається стрімка зміна режиму надання публічних (державних) послуг з фізичного на електронний, унаслідок чого урядам доводиться функціонувати як цифровим платформам, що надають послуги, а також інфраструктуру для інших інформаційних систем, керованих ІТ.

1 INTOSAI-P 1 «Лімська декларація».

2 Резолюція Генеральної Асамблеї Організації Об'єднаних Націй A/66/209.

1.5 Перехід до комп'ютеризованих інформаційних систем та електронної обробки даних об'єктами аудиту в публічному (державному) секторі спричинив значні зміни в середовищі, в якому працюють ВОА. Витрати публічного (державного) сектора на ІТ зростають. Існує також потреба забезпечити впровадження суб'єктами (публічного) державного сектору внутрішнього контролю за ІТ для підтримання конфіденційності, цілісності та доступності даних. Отже, для ВОА стає вкрай необхідно розвивати відповідну спроможність проводити ретельну перевірку заходів контролю, пов'язаних з інформаційними системами.

2

МЕТА ЦЬОГО GUID

2.1 ISSAI 100, 200, 300 і 400 містять основні принципи аудиту, застосовні до фінансового аудиту, аудиту діяльності та аудиту відповідності. Ці ISSAI стосуються загальних принципів, процедур, стандартів та очікувань аудитора. Вони також застосовні й до аудиту інформаційних систем.

2.2 Метою цього GUID є надання аудиторам керівництва щодо того, як проводити аудити діяльності та/або відповідності, пов'язані з конкретним предметом аудиту інформаційних систем, або, коли аудит інформаційних систем може бути частиною більшого аудиторського завдання з проведення фінансового аудиту, аудиту відповідності чи аудиту діяльності.

2.3 Вміст цього GUID може застосовуватися аудиторами на етапах планування, виконання, звітування та контролю виконання рекомендацій [3] процесу аудиту.

[3] ISSAI 100.

3

ВИЗНАЧЕННЯ

3.1 Інформаційні системи: Інформаційні системи можна визначити як поєднання стратегічної, управлінської та операційної діяльності, пов'язаної зі збиранням, обробленням, зберіганням, поширенням і використанням інформації, та пов'язаних з нею технологій. Складність такої інформаційної системи може варіюватися від простої книги, куди вручну вносять записи про отримання та сплату грошей, до більш складної системи, керованої ІТ, як-от система нарахування податків, у якій автоматизовано всі процеси – збирання даних (наприклад, податкові декларації, подані через онлайн-вебпортал), зберігання на серверах, нарахування податків (на основі програмування з використанням правил оподаткування) та доведення податкових вимог, відшкодування та підтвердження (у реальному часі або через встановлені проміжки часу). Інформаційна технологія охоплює апаратне забезпечення, програмне забезпечення, комунікаційні та інші засоби, що використовуються для введення, зберігання, оброблення, передачі та виведення даних у будь-якій формі.

3.2 Аудит інформаційних систем можна визначити як перевірку заходів контролю, пов'язаних з інформаційними системами, керованими ІТ, для виявлення випадків відхилення від критеріїв, які, у свою чергу, було визначено на основі типу аудиторського завдання: тобто фінансового аудиту, аудиту відповідності чи аудиту діяльності.

4

СФЕРА ЗАСТОСУВАННЯ

4.1 Аудитори можуть користуватися цим GUID для проведення аудитів діяльності та/або відповідності щодо конкретного предмета аудиту інформаційних систем, а також там, де аудит інформаційних систем є частиною більшого аудиторського завдання, яке може полягати у фінансовому аудиті, аудиті відповідності та/або аудиті діяльності.

4.2 Це керівництво подає подальші настанови щодо того, як може проводитись аудит інформаційних систем шляхом фінансового аудиту/аудиту діяльності та аудиту відповідності, й не містить жодних подальших вимог щодо проведення аудиту.

5

ПЛАНУВАННЯ АУДИТУ

5.1 ВОА можуть застосовувати для аудиту ІС планування аудиту на основі ризиків відповідно до процесу, описаного в ISSAI 100, ISSAI 200 (для фінансового аудиту), ISSAI 300 (для аудиту діяльності) та ISSAI 400 (для аудиту відповідності), залежно від цілей завдання з аудиту.

5.2 Робота з аудиту інформаційних систем визначатиметься метою та обсягом аудиту. Ось кілька прикладів:

1) оцінити відповідні загальні заходи контролю[4] та прикладні заходи контролю,[5] що впливають на достовірність даних з інформаційних систем, що, у свою чергу, впливає на фінансову звітність об'єкта аудиту;

2) отримати впевненість у відповідності процесів інформаційних систем законам, політикам і стандартам, застосовним до об'єкта аудиту;

3) отримати впевненість у тому, що ІТ-ресурси забезпечують ефективне та результативне досягнення цілей організації, а відповідні загальні заходи контролю та прикладні заходи контролю є ефективними в запобіганні, виявленні та виправленні випадків надмірності, марнотратства та неефективності у використанні та управлінні інформаційними системами.

[4] Загальні заходи контролю — це ручні або автоматизовані процедури, спрямовані на забезпечення конфіденційності, цілісності та доступності інформації у фізичному середовищі, в якому розробляються, підтримуються та експлуатуються інформаційні системи.

[5] Прикладні заходи контролю — це ручні або автоматизовані процедури в межах інформаційної системи, яка впливає на оброблення транзакцій, і вони можуть бути пов'язані з перевіркою вхідних даних, точним обробленням даних, доставленням вихідних даних, і з заходами контролю за цілісністю основних даних (майстер-даних).

5.3 Обсяг аудиту ІС, що визначається на основі оцінки ризику, може формуватися з будь-якої або всіх зазначених нижче сфер[6] об'єкта аудиту:

1) організаційна політика щодо ІТ[7];
2) організаційна структура управління з питань ІТ;
3) загальні заходи контролю, передбачені в бізнес-сфері, що автоматизується;
4) управління активами;
5) розробка, придбання та супровід інформаційних систем, включно з відображенням бізнес-процесів і відповідної логіки програмування;
6) управління ІТ-діяльністю;
7) управління фізичним середовищем;
8) управління людськими ресурсами;
9) управління комунікацією;
10) управління інформаційною безпекою[8];
11) управління дотриманням вимог законодавства;
12) безперервність діяльності та управління аварійним відновленням;
13) управління прикладними заходами контролю.

5.4 Визначаючи обсяг аудиту для аудиторського завдання щодо інформаційних систем, ВОА можуть обрати для аудиторського аналізу певний період часу (наприклад один рік, три роки тощо). Можна обирати відповідний проміжок часу, який є доречним, зважаючи на цілі аудиторського завдання.

5.5 Якщо аудит інформаційних систем є частиною аудиторського завдання, ВОА можуть забезпечувати комплексну роботу команди з аудиту щодо досягнення загальної мети аудиту. Для забезпечення ефективної інтеграції ВОА можуть розглянути можливість:

1) ретельного документування роботи, яку мають виконати аудитори інформаційних систем;
2) створення протоколу обміну інформацією між аудиторами інформаційних систем та іншими аудиторами;
3) визначення того, які інформаційні системи та цілі контролю належать до обсягу аудиту.

6 Більшість описаних сфер адаптована до ISO/IEC 27001.
7 Включно з аспектами стратегічного менеджменту.
8 Включно з кібербезпекою.

5.6 ВОА можуть забезпечити формування команди з аудиту в такий спосіб, щоб її учасники разом мали компетенцію виконувати завдання з аудиту інформаційних систем для досягнення цілей аудиту.

5.7 Відповідно до стратегічного плану ВОА необхідні знання, навички та компетентність можуть бути здобуті шляхом поєднання навчання, добору та залучення зовнішніх ресурсів.

5.8 ВОА можуть забезпечувати наявність у команд з аудиту інформаційних систем колективної спроможності:

1) розуміти технічні елементи інформаційної системи, керованої ІТ, включно з усіма відповідними екземплярами використовуваної програми, щоб мати змогу одержувати доступ до ІТ-інфраструктури та використовувати її для процесу аудиту;
2) розуміти чинні правила, норми та середовище, в якому в об’єкта аудиту працюють інформаційні системи, керовані ІТ;
3) розуміти відображення бізнес-процесів у логіці програмування для інформаційної системи об’єкта аудиту;
4) застосовувати знання бізнесу та ІТ для оцінювання ризику ручного керування системною програмою чи конфігурацією, що уможливило б обробку нетипових транзакцій;
5) оцінювати структуру і перевіряти операційну ефективність прикладних заходів контролю у відповідних інформаційних системах;
6) розуміти методологію аудиту, включно з відповідними стандартами аудиту та керівництвами, застосовними до ВОА;
7) розуміти критерії ефективності діяльності/відповідності у сфері ІТ, з якими слід порівнювати результати аудиту, включно з такими структурами управління інформаційними системами, як COBIT, ITIL, TOGAF;
8) розуміти методи у сфері інформаційних систем для збирання аудиторських доказів з автоматизованих систем;
9) розуміти Інструменти аудиту інформаційних систем для збирання, аналізу та відтворення результатів такого аналізу або повторного виконання перевірених аудитом функцій;
10) отримувати доступ до Інфраструктури інформаційних систем і використовувати її для фіксації та збереження аудиторських доказів;
11) отримувати доступ до Інструментів аудиту інформаційних систем і використовувати їх для аналізу зібраних доказів.

5.9 ВОА можуть розглядати різні варіанти розподілу людських ресурсів для виконання завдань з аудиту інформаційних систем. До їх числа можуть належати створення центральної групи фахівців з ІТ, які допомагатимуть іншим командам з аудиту в ВОА проводити ці аудити, або залучення фахівців з ІТ відповідно до вимог. Зі збільшенням кількості виконаних завдань з аудиту інформаційних систем ВОА можуть розглянути можливість створення спеціалізованої групи або служби аудиту інформаційних систем. Цій групі може бути доручене виконання всіх завдань з аудиту інформаційних систем для ВОА; вона може взаємодіяти з іншими командами ВОА, які мають успадковані знання про об'єкт аудиту, щоб швидко розбиратися у функціях суб'єкта та відповідних бізнес-процесах. Оскільки технологія дедалі більше інтегрується в інформаційні системи, ВОА можуть забезпечувати здобуття всіма аудиторами відповідних навичок проведення аудиту інформаційних систем.

5.10 У разі обмеженості ресурсів ВОА можуть залучати зовнішні ресурси, як-от консультантів з ІТ, виконавців, фахівців та експертів для проведення аудиту інформаційних систем. ВОА можуть стежити за тим, щоб такі зовнішні ресурси були належно підготовлені та ознайомлені з інструкціями щодо професійної поведінки та з процесами й продуктами аудиту інформаційних систем, які застосовуються до ВОА, а також щоб їхня робота належно контролювалася за допомогою документально оформленого контракту чи угоди про рівень обслуговування й відповідного залучення персоналу ВОА до етапів планування, проведення, звітування та контролю виконання рекомендацій аудиту. Отже, ВОА можуть потребувати кваліфікованих і обізнаних членів власної команди для моніторингу роботи зовнішніх ресурсів і забезпечення дотримання інструкцій і угод про рівень обслуговування.

5.11 Для проведення оцінки ризиків для завдань з аудиту інформаційних систем аудитори можуть використовувати принципи, викладені в ISSAI 100, 200, 300 і 400, на додачу до тих, що використовуються для перевірки конкретного предмета аудиту інформаційних систем, які викладено нижче:

1) невід'ємний ризик полягає в імовірності того, що певні характеристики керованих ІТ інформаційних систем об'єкта аудиту за своєю природою можуть несприятливо впливати на виконання функції, яку має виконувати суб'єкт. Наприклад, інформаційна система об'єкта аудиту, від якої вимагається надання інформації для всіх представників громадськості, містить невід'ємний ризик продуктивності, який полягає в тому, що після перевищення очікуваної граничної пікової кількості користувачів інформаційна система може не відповідати, а інформація виявиться недоступною для будь-якого користувача. Попри те, що об'єкт аудиту може застосовувати заходи контролю для пом'якшення невід'ємних ризиків, у багатьох випадках об'єкт аудиту може бути змушений просто змиритися з існуванням таких ризиків у межах прийнятного рівня ризику. Невід'ємний ризик може бути оцінений до того, як аудитори розглянуть вплив ризику контролю або невиявлення;

2) ризик контролю для інформаційної системи складатиметься з імовірності того, що заходи контролю ІТ, які були впроваджені об'єктом аудиту, можуть не зменшити несприятливого впливу, якому вони мали протидіяти. Наприклад, інформаційна система об'єкта аудиту, яка повинна гарантувати, що доступ до конфіденційних даних обмежений уповноваженим персоналом, може запровадити захід контролю, як-от вимога до персоналу, який намагається отримати доступ, зазначати ім'я користувача та пароль. Ризик контролю в цій ситуації полягає у відсутності належного захисту імені користувача та паролю, адже вони можуть бути вгадані неуповноваженим персоналом після неодноразових спроб введення, що призведе до втрати конфіденційності та потенційного негативного впливу на об'єкт аудиту. Об'єкт аудиту, який наполягає на використанні безпечних нетривіальних паролів, що містять комбінацію літер, цифр і спеціальних символів, і гарантує, що інформаційна система заборонить доступ до імені користувача після певної кількості невдалих спроб отримати доступ, матиме нижчий ризик контролю, ніж той, який не має цих функцій;

3) ризик невиявлення складається з імовірності того, що аудитор не виявить відсутності, несправності чи неадекватності заходів контролю ІТ, запроваджених організацією, що може мати потенційно негативний вплив на суб'єкта.

5.12 Для проведення оцінок систем, керованих ІТ, на основі ризиків, ВОА можуть обрати методологію, яка відповідає їхньому призначенню. Такі методології можуть варіюватися від простих класифікацій профілю ризику ІТ-середовища об'єкта аудиту за принципом «високий», «середній» і «низький» на основі того, як ВОА розуміють об'єкт аудиту та його середовище, та професійного судження команди з аудиту інформаційних систем ВОА, до складніших розрахунків, які кількісно оцінюють рейтинг ризику на основі об'єктивних даних, зібраних у об'єкта аудиту.[9]

5.13 Рішення про суттєвість питання аудиту інформаційних систем може бути ухвалене відповідно до загальної основи визначення суттєвості, прийнятої ВОА. Перспектива щодо суттєвості може відрізнятися залежно від характеру завдання з аудиту інформаційних систем. Суттєвість для фінансового аудиту, аудиту діяльності та відповідності в державному секторі, на основі якої розроблятиметься завдання з аудиту інформаційних систем, описано в ISSAI 100, 200, 300 та 400.[10]

---

9 *Посібник з аудиту інформаційних технологій для вищих органів аудиту, розроблений Робочою групою з аудиту інформаційних технологій (WGITA) та Ініціативою з розвитку INTOSAI (IDI).*

10 ISSAI 200 *«Принципи фінансового аудиту»,* ISSAI 300 *«Принципи аудиту діяльності»,* ISSAI 400 *«Принципи аудиту відповідності».*

6

ПРОВЕДЕННЯ АУДИТУ

6.1 ВОА можуть проводити аудит інформаційних систем відповідно до процесу, описаного для завдань з фінансового аудиту (ISSAI 200), аудиту діяльності (ISSAI 300) та аудиту відповідності (ISSAI 400), залежно від характеру завдання.

6.2 Спеціально для аудиту інформаційних систем аудитори можуть вимагати від об'єкта аудиту належної співпраці та підтримки в проведенні аудиту, включно з доступом до записів та інформації. Аудитори можуть визначати режим доступу до електронних даних у форматі, необхідному для проведення аналізу, за узгодженням з об'єктом аудиту. Режим доступу до даних буде специфічним для ВОА.

6.3 Перед початком оцінювання заходів контролю в інформаційній системі аудитори можуть сформувати розуміння архітектури системи, базових даних та їх джерел, щоб визначити необхідні інструменти та методи аудиту.

6.4 У разі отримання від об'єкта аудиту дампів даних[11] аудитори можуть стежити за тим, щоб кожен дамп даних супроводжувався листом від об'єкта аудиту. Такий супровідний лист може містити:

1) джерело даних (через посилання на мітку часу створення дампу даних/хеш-число дампу даних) для забезпечення цілісності даних, автентифікації[12] й неможливості спростування[13] факту одержання;

2) параметри екстракції, використані для створення дампу даних, тобто використані запити/запущені звіти;

3) якщо такий супровідний лист від об'єкта аудиту не отримано,

---

11 Дамп даних — це великий обсяг даних, що передається з однієї системи або одного місця в іншу систему або інше місце.

12 Автентифікація — це акт перевірки ідентичності користувача — глосарій термінів Асоціації аудиту і контролю інформаційних систем (ISACA).

13 Неможливість спростування факту одержання — це гарантія того, що сторона пізніше не зможе спростувати факт формування даних; надання доказів цілісності та походження даних, які можуть бути перевірені третьою стороною — глосарій термінів Асоціації аудиту і контролю інформаційних систем (ISACA).

аудитори можуть сформувати внутрішні документи з зазначенням важливої інформації, як-от дати передання даних, файлу, з якого було створено дамп даних, і того, чи дані надійшли з експлуатаційного чи з якогось іншого середовища тощо.

6.5 Аудитори можуть провести оцінку заходів контролю ІТ (загальних та прикладних заходів контролю), запроваджених об'єктом аудиту, щоб перевірити їхню надійність і достатність. Оцінку можна провести за допомогою відповідної комбінації таких методів: інтерв'ю, анкетування, спостереження, прогін програми, блок-схеми, збирання та аналіз даних, верифікація, повторне обчислення, повторне оброблення та підтвердження третьою стороною. Обсяг оцінювання заходів контролю може включати перевірку таких аспектів:

1) політику щодо інформаційних систем визначено, прийнято та повідомлено;
2) структура управління інформаційними системами впроваджена та функціонує;
3) інвентаризація активів інформаційних систем проводилася періодично й було визначено вимоги до розширення, заміни та видалення;
4) процеси спільного використання інфраструктури та загальних служб інформаційних систем з іншими публічними (державними) суб'єктами впроваджені та функціонують;
5) процеси розробки, придбання та супроводу інформаційних систем було визначено, прийнято та повідомлено (включно з процесом управління змінами);
6) процеси експлуатації ІТ (залучення власних працівників, аутсорсинг, угоди про надання послуг) визначено, ухвалено та повідомлено;
7) вжито заходів щодо гарантування фізичної безпеки й передбачених фізичних умов праці;
8) вжито заходів щодо навчання та підвищення обізнаності людських ресурсів для забезпечення конфіденційності, цілісності й доступності інформації, та дотримання вимог політики щодо інформаційних систем і структури управління;
9) вжито заходів щодо забезпечення конфіденційності, цілісності та доступності різних режимів і каналів зв'язку;
10) вжито заходів щодо управління інформаційною безпекою;

11) вжито заходів щодо управління дотриманням законодавства;

12) вжито заходів щодо безперервності діяльності та управління аварійним відновленням;

13) прикладні заходи контролю, прийняті у кожній інформаційній системі, є адекватними й надійними. Така оцінка може передбачати ідентифікацію важливих компонентів програм, визначення критичності програми для суб'єкта господарювання, розгляд наявної документації, інтерв'ю з персоналом, розуміння ризиків прикладних заходів контролю та їх впливу на суб'єкта господарювання, а також розробку тестів для перевірки таких прикладних заходів контролю на адекватність і надійність.

6.6 Отже, оцінка загальних і прикладних заходів контролю може охоплювати політику, процеси, людей і системи об'єкта аудиту відповідно до цілей аудиту інформаційних систем.

6.7 Залежно від мети аудиту, аудитори можуть бути занепокоєні з приводу розробки, впровадження та операційної ефективності заходів контролю. Якщо аудитора непокоїть структура заходів контролю, то може бути достатньо провести інтерв'ю чи перевірити задокументовані бізнес-правила. Якщо аудитора непокоїть реалізація заходів контролю, то запиту може бути недостатньо, відповідно, може постати потреба у проведенні покрокового прогону або виконанні аналізу даних для підтвердження того, що захід контролю було реалізовано в тому вигляді, в якому його було побудовано. Насамкінець, якщо аудитора непокоїть операційна ефективність заходу контролю, може постати потреба в тестуванні вибірки операцій для демонстрації того, що протягом відповідного періоду захід контролю діяв ефективно.

6.8 Аудитори можуть також розглянути те, у який спосіб докази щодо загальних заходів контролю впливають на характер, час і обсяг доказів, необхідних для отримання впевненості щодо функціонування прикладних заходів контролю. Якщо аудитор отримав достатні та прийнятні аудиторські докази ефективності загальних заходів контролю, які підтримують логічний доступ персоналу до ІТ-систем і управління змінами в експлуатаційному середовищі, аудитор має змогу дійти висновку про операційну ефективність автоматизованих процедур прикладного контролю. Це можна зробити шляхом тестування меншої вибірки транзакцій, оскільки ефективність загального ІТ-середовища надає аудиторові докази ефективності прикладного контролю у відповідний період. У разі застосування ручних процедур прикладного контролю у аудиторів може виникнути необхідність тестування розміру вибірки, що відповідає обраному рівню впевненості.

6.9 На підставі оцінки заходів контролю ІТ аудитори можуть визначити пріоритетні напрями проведення тестування по суті, яке передбачає детальне тестування заходів контролю ІТ за допомогою різних методів автоматизованого аудиту (CAAT) для формування запитів, екстракції та аналізу даних. Аудитори можуть розробити та виконати тестування по суті для обґрунтування цілей аудиту. Аудитори можуть обирати відповідні методи автоматизованого аудиту на основі своїх вимог.

6.10 Аудитори можуть використовувати автоматизований аудит для використання таких методів аудиту інформаційних систем, як аналіз журналів користувачів, формування повідомлень про виняткові ситуації, підрахунок за полями, порівняння файлів, стратифікація, вибірка, перевірки на наявність дублікатів, виявлення прогалин, застарівання, обчислення за віртуальними полями тощо. До переваг використання методів автоматизованого аудиту належать аналіз великих обсягів даних, повторюваність тестів на різних наборах даних і з різними критеріями та автоматизоване документування тестів і результатів аудиту з мітками часу.

6.11 Аудитори не завжди мають змогу перевірити всі екземпляри, транзакції, модулі чи системи ІТ з огляду на обмеженість ресурсів і необхідність балансу між витратами на аудит і користю від нього. Зважаючи на міркування суттєвості, ВОА в такій ситуації можуть прийняти аудиторську вибірку для детального дослідження, щоб дійти обґрунтованих аудиторських висновків. ВОА можуть використовувати відповідні методи автоматизованого аудиту для виконання різних типів формування вибірки й визначати відповідний розмір вибірки залежно від базових невід'ємних ризиків і ризиків контролю. Аудиторські вибірки [14] формуються для того, щоб надати аудиторові обґрунтовану основу для висновків щодо всієї сукупності даних на підставі висновків, зроблених у результаті застосування аудиторських процедур та аналізу аудиторської вибірки. Аудитори можуть враховувати мету аудиторської процедури та характеристики генеральної сукупності, з якої буде здійснюватися вибірка, та визначати розмір вибірки, достатній для зменшення ризику вибірки в межах прийнятного рівня. Аудит у середовищі ІТ може полегшити аналіз 100 відсотків сукупності, особливо на етапі попереднього оцінювання. Однак вибірки можуть знадобитися для проведення тестування по суті. Формуючи вибірку в межах фінансового аудиту, аудитори інформаційних систем можуть застосовувати для добору вибірки ISSAI 2530 .[15]

6.12 Аудитори можуть переконуватися в тому, що зібрані та задокументовані електронні докази є достатніми, надійними та точними для підтвердження аудиторських спостережень. Такі електронні докази можуть складатися з файлів даних, журналів користувачів, аналітичних моделей,

[14] ISSAI 2530 *«Фінансовий аудит, формування аудиторської вибірки»*, розділи з 6 по 9

[15] ISSAI 2530 *«Фінансовий аудит, формування аудиторської вибірки»*, розділи з 6 по 9.

звітів інформаційних систем управління тощо, й можуть бути зібрані та збережені в належний спосіб так, щоб вони були доступні для забезпечення впевненості у точності та достовірності процесу аудиту. Докази, зібрані під час аудиту інформаційних систем, можуть мати необхідні мітки часу та детальні відомості, що містять етапи виконаного аналізу даних, щоб було ясно, коли відповідні докази були створені, збережені та змінені востаннє, щоб знизити ризик їх зміни в подальшому.

6.13 Документацію з аудиту інформаційних систем можна зберігати та захищати від будь-яких змін і несанкціонованого видалення. ВОА можуть розробити нові стандарти для зберігання документації з аудиту інформаційних систем або адаптувати існуючі стандарти до виконання вимог щодо зберігання документації, пов'язаної з аудитом інформаційних систем. Визначений у такий спосіб період зберігання залежатиме від повноважень окремих ВОА та закону (законів), що регулюють їх діяльність. Особлива увага може приділятися носіям, формату, очікуваному строку зберігання та вимогам до зберігання цих даних, щоб гарантувати доступність даних для читання протягом строку, встановленого політикою кожного з ВОА зі зберігання та архівування даних. Це може зумовлювати необхідність конвертації даних з одного формату в інший, щоб іти в ногу з технологічним прогресом і уникнути застарівання технологій.

6.14 У разі перевірки технічних звітів, складених сторонніми аудиторами, з предметів аудиту, що стосуються певних технологій, аудитори можуть застосовувати відповідні процедури для отримання впевненості щодо аспектів відповідності, фінансових аспектів або аспектів діяльності з таких звітів.[16] Якщо в результаті таких процедур аудитор покладається на зміст таких звітів, факт покладання на них може бути у відповідний спосіб розкритий.

6.15 Стандарти ISSAI зазначають, що аудитори повинні налагоджувати ефективну комунікацію впродовж усього процесу аудиту та інформувати об'єкт аудиту про всі питання, пов'язані з аудитом (див. параграф 43 ISSAI 100). Під час аудитів, до складу яких входить робота з аудиту інформаційних систем, результати аудиту інформаційних систем у деяких випадках можуть бути повідомлені об'єкту аудиту окремим листом. У цих випадках важливо пояснити, як саме результат аудиторської роботи пов'язаний з іншими повідомленнями в межах того самого фінансового аудиту, аудиту діяльності або відповідності, і як саме результати роботи з аудиту інформаційних систем можуть бути доречні для підсумкового аудиторського звіту ВОА.

[16] Якщо обсяг аудиту перебуває в межах фінансового аудиту, аудитори можуть використовувати ISSAI 2402 *«Положення щодо аудиту суб'єкта господарювання, що користується послугами організації, що надає послуги»*.

7

ЗВІТУВАННЯ ПРО АУДИТ

7.1 Оскільки завдання з аудиту інформаційних систем буде або фінансовим аудитом (ISSAI 200), аудитом діяльності (ISSAI 300) або аудитом відповідності (ISSAI 400), аудитори можуть розглядати вимоги до звітування у відповідний спосіб. Він буде специфічним для ВОА. Подібно до цього, кожен з ВОА може мати власні граничні рівні звітування, визначені на основі суттєвості результатів аудиту. Так само аудитор, звітуючи про завдання з аудиту інформаційних систем, може враховувати законодавчі та внутрішні обмеження щодо розкриття фінансової та технічної інформації.

7.2 Аудитори мають знати про необхідність обмеження використання технічної мови та делікатний характер поданої у звіті інформації (наприклад паролів, імен користувачів, ідентифікаторів та особистої інформації). Попри технічний характер аудиту інформаційних систем аудитори можуть стежити за тим, щоб звіт був повністю зрозумілий для вищого управлінського персоналу об’єкта аудиту, зацікавлених сторін і широкої громадськості. Аудитори можуть включати детальний глосарій термінів до звітів, які містять перехресні посилання на визначення абревіатури чи терміна з поясненням того, як вони працюють у середовищі контролю, на основі сценарію.

7.3 Аудитори мають урахувати потенційний негативний вплив звіту після публікації звіту про аудит інформаційних систем. Наприклад, якщо у звіті про аудит інформаційних систем виявлено певні ризики безпеки в інформаційній системі об’єкта аудиту, і про них повідомляється ще до того, як буде запроваджено заходи контролю, необхідні для зниження ризиків, то громадськість може дізнатися про уразливість інформаційної системи. За таким сценарієм аудитори можуть розглянути такі варіанти, як звітування лише після запровадження необхідних заходів контролю чи відмова від звітування про конкретний безпековий ризик у повному обсязі, щоб уникнути потенційного несприятливого впливу на об’єкт аудиту.

8

КОНТРОЛЬ ВИКОНАННЯ РЕКОМЕНДАЦІЙ

8.1 Оскільки завдання з аудиту інформаційних систем спирається на один чи декілька основних типів аудиту, аудитори можуть вважати, що вимоги до контролю за дотриманням норм для таких завдань з аудиту відповідають вимогам для фінансового аудиту (ISSAI 200), аудиту діяльності (ISSAI 300) та аудиту відповідності (ISSAI 400).