МІЖНАРОДНИЙ СТАНДАРТ
ISO

37001

Перше видання 2016-10-15

Системи управління протидією хабарництву – Вимоги та посібник із використання

Anti-bribery management systems—Requirements with guidance for use

Код посилання
ISO 37001:2016(E)

© ISO 2016

ДОКУМЕНТ ЗАХИЩЕНО АВТОРСЬКИМ ПРАВОМ

© ISO 2016, Опубліковано у Швейцарії

Усі права зберігаються. За винятком окремих зазначених випадків, жодна з частин даного документу не підлягає копіюванню або використанню в будь-якій іншій формі або будь-яким електронним чи механічним чином, включаючи фотокопії та записи в Інтернеті або електронних системах внутрішніх мереж без попередньої письмової згоди. Відповідну згоду можна отримати від Міжнародної організації зі стандартизації (ISO) за запитом, поданим за приведеною нижче адресою? або від комітет-члена ISO в країні особи, яка подає відповідний запит.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Передмова.....v

Вступ .....

vi 1 Сфера застосування.....1 2

Нормативні посилання.....1 3

Термінологія і визначення.....1

4 Контекст організації.....6 4.1.
Розуміння організації та її контексту .....6 4.2.
Розуміння потреб та очікувань зацікавлених сторін.....6 4.3.
Визначення сфери застосування системи управління протидією хабарництву ..6 4.4.
Система управління протидією хабарництву .....7 4.5.
Оцінка ризику хабарництва 7

5 Керівництво.....8 5.1.
Керівництво та зобов'язання .....8 5.1.1. Керівний орган.....8 5.1.2. Вище керівництво.....8 5.2. Політика протидії хабарництву.....9 5.3. Організаційні функції, відповідальність та повноваження.....9 5.3.1. Функції та відповідальність.....9 5.3.2. Підрозділ забезпечення нормативно-правової відповідності .....10 5.3.3. Делегування ухвалення рішень 10

6 Планування.....10 6.1.
Діяльність стосовно ризиків та можливостей.....10 6.2.
Цілі протидії хабарництву та планування з їх досягнення.....11

7 Підтримка .....11 7.1.
Ресурси.....11 7.2.
Компетентність.....12
7.2.1. Загальні положення.....12 7.2.2. Процес найму.....12 7.3.
Інформування та навчання.....13 7.4.
Комунікація.....13 7.5.
Задокументована інформація .....14 7.5.1. Загальні положення.....14 7.5.2. Створення й поновлення.....14 7.5.3. Контроль задокументованої інформації.....14

8 Функціонування.....15 8.1.
Оперативне планування й контроль.....15 8.2.
Комплексна перевірка («Due diligence»).....15 8.3.
Фінансовий контроль .....16 8.4.
Не-фінансовий контроль .....16 8.5.
Здійснення контролю протидією хабарництву підконтрольними організаціями й діловими партнерами .....16 8.6.
Зобов'язання щодо протидії хабарництву .....17 8.7.
Подарунки, прояви гостинності, пожертви та аналогічні внески.....17 8.8.
Управління у випадку невідповідності контролю протидією хабарництву .....17 8.9.
Тривожні сигнали.....17 8.10.
Розслідування та вирішення проблем хабарництва.....18

9 Оцінка виконання.....18 9.1.
Моніторинг, вимірювання, аналіз та оцінка .....18 9.2. Внутрішній аудит.. .....19 9.3. Аналіз збоку керівництва. .....20 9.3.1. Аналіз збоку вищого керівництва 20

© ISO 2016 – All rights reserved

9.3.2. Аналіз збоку керівного органу 20
9.4. Аналіз збоку Підрозділу забезпечення нормативно-правової відповідності.....21
10 Удосконалення.....21
10.1. Невідповідність та коригування.....21
10.2. Постійне вдосконалення 22
Додаток А (інформативний) **Посібник із використання даного документу.....23**
Бібліографія.....46

© ISO 2016 – Усі права зберігаються

МІЖНАРОДНИЙ СТАНДАРТ ISO 37001:2016(E) Передмова

ISO (Міжнародна організація зі стандартизації) – це світова федерація національних органів стандартизації (комітет-члени ISO). Робота з підготовки міжнародних стандартів зазвичай проводиться технічними комітетами ISO. Кожний комітет-член, зацікавлений у тематиці, заради якої було створено той чи інший технічний комітет, має право на представництво в такому комітеті. У роботі організації також беруть участь міжнародні організації, урядові й неурядові. ISO тісно співпрацює з Міжнародною Електротехнічною комісією (МЕК/IEC) з усіх питань електротехнічної стандартизації.

Процедури, що їх було використано для створення даного документу та призначено для його подальшого доопрацювання, описані в Директивах ISO/IEC, Частині 1. Зокрема різні типи документів ISO потребують різних критеріїв затвердження, і на це слід зважати. Цей документ було розроблено відповідно до правил редагування Директив ISO/IEC, Частини 2 (див. www.iso.org/directives).

Слід звернути увагу на можливість того, що певні елементи даного документу можуть підпадати під патентні права. ISO не несе відповідальності за визначення жодних таких прав. Детальну інформацію стосовно будь-яких патентних прав, визначених протягом підготовки даного документу, можна знайти у Вступі і/або списку патентних декларацій, отриманих ISO (див. www.iso.org/patents).

Будь-які торгові марки, використані в рамках даного документу, приводяться виключно з інформативною метою для зручності користування ним, і це не повинні сприйматися в якості підтримки таких торгових марок.

Для отримання пояснень щодо значень певної специфічної термінології і виразів ISO стосовно оцінки відповідності й інформації про дотримання організацією ISO принципів Всесвітньої торгової організації (далі, також «ВТО») щодо технічних бар'єрів у торгівлі (далі, також «ТБТ»), зверніться за наступним посиланням: www.iso.org/iso/foreword.html.

Комітет, відповідальний за цей документ – це Проектний комітет ISO/PC 278 («Системи управління протидією хабарництву»).

МІЖНАРОДНИЙ СТАНДАРТ ISO 37001:2016(E) Вступ

Хабарництво – це широко відоме явище. Його можна вважати причиною низки серйозних соціальних, моральних, економічних та політичних проблем, воно підриває довіру до процесів належного урядування, заважає розвитку та деформує процес конкурентної боротьби. Воно руйнує авторитет правосуддя, ставить під сумнів права людини та вважається перепоною для боротьби з бідністю. Це явище також підвищує вартість ведення бізнесу, додає непевності до комерційних правочинів, збільшує вартість товарів і послуг, знижує якість продукції й послуг, що може призвести до втрати життя і власності, знищує довіру до державних інституцій та втручається до процесу чесної й ефективної роботи ринків.

Урядам різних країн вдалося досягти певного прогресу у вирішенні проблеми хабарництва шляхом укладання міжнародних угод, як наприклад Конвенція з боротьби з підкупом посадових осіб іноземних держав у разі проведення міжнародних ділових операцій Організації економічної співпраці й розвитку[15] та Конвенція Організації об'єднаних націй проти корупції[14], а також національного законодавства. У більшості юрисдикцій участь в акції хабарництва для фізичної особи вважається злочином, і спостерігаються наростаюча тенденція до притягнення до відповідальності фізичних осіб та організації, причетних до хабарництва.

Проте самого лише закону недостатньо для вирішення цієї проблеми. Організації повинні брати активну участь у процесі боротьби з хабарництвом. Цього можна досягти шляхом застосування системи управління протидією хабарництву, надання якої ставиться за мету даним документом, а також шляхом зобов'язань керівництва щодо створення культури доброчесності, прозорості, відкритості й відповідності. Природа організаційної культури критично важлива для успіху або невдачі з використанням системи управління протидією хабарництву.

Від належним чином керованої організації очікується готова політика відповідності за підтримки належних систем управління для допомоги з дотриманням відповідності зобов'язанням організації

стосовно права та доброчесності. Політика протидії хабарництву вважається компонентом загальної політики відповідності. Політика протидії хабарництву та система управління на підтримку такій політиці допомагає організації уникнути або мінімізувати витрати, ризики й збитки від участі в процесі хабарництва, просувати ідеї довіри й упевненості в правочинах та покращити свою репутацію.

У даному документі приведена краща міжнародна практика, і його можна використовувати для всіх юрисдикцій. Він застосовується до малих, середніх та великих організацій усіх секторів, включаючи державний, приватний і неприбутковий. Ризики хабарництва, з якими стикається організація, відрізняються залежно від таких факторів, як розмір організації, розташування й сфери, у якій працює організація, а також природи, масштабу та складності діяльності організації. Даним документом визначається реалізація організацією її політики, процедур та здійснення контролю, які вважаються обґрунтованими й пропорційними стосовно ризиків хабарництва, з якими стикається організація. У Додатку А подано посібник із реалізації вимог цього документу.

Відповідність даному документу не дає жодних гарантій відсутності випадків хабарництва в минулому чи майбутньому стосовно конкретної організації, адже цілковито усунути ризик хабарництва неможливо. Проте цей документ може допомогти організації вжити обґрунтованих і пропорційних заходів на упередження, виявлення й реагування на випадки хабарництва.

У рамках даного документу використовуються наступні дієслівні форми: —

«повинен»/«зобов'язаний»/«необхідно» вказує на вимогу;

— «слід»/«мав би» вказує на рекомендацію;

— «може» або «дозволяється» вказує на дозвіл;

 — «спроможний»/«мати можливість»

вказує на можливість або здатність.

Інформація, відмічена як «ПРИМІТКА», вноситься в якості настанов для кращого розуміння чи роз'яснення відповідної вимоги.

Даний документ відповідає вимогам ISO до стандартів системи управління. Такі вимоги включають у себе структуру високого рівня, ідентичний основний текст та загальні терміни базових визначень, які розроблено для зручності користувачів із реалізацією численних стандартів систем управління ISO. Цим документом можна користуватися в поєднанні з іншими стандартами систем управління (наприклад, ISO 9001, ISO 14001, ISO/IEC 27001 і ISO 19600) та стандартами управління (наприклад, ISO 26000 та ISO 31000).

МІЖНАРОДНИЙ СТАНДАРТ ISO 37001:2016(E)

Системи управління протидією хабарництву - Вимоги та посібник із використання

1 Сфера застосування

У даному документі приведено вимоги й настанови зі створення, реалізації, обслуговування, перегляду й удосконалення системи управління протидією хабарництву. Така система може бути автономною або ж інтегрованою до загальної системи управління. Даний документ зважає на наступне в контексті діяльності організації:

— хабарництво в державному, приватному й неприбутковому секторах; —

хабарництво збоку організації;

— хабарництво збоку персоналу організації, який виступає від імені такої організації та в її інтересах;

— хабарництво збоку ділових партнерів організації, які виступають від імені такої організації та в її інтересах;

— хабарництво в організації;

— хабарництво, що чиниться персоналом організації стосовно діяльності такої організації; —

хабарництво в рамках ділових партнерів організації стосовно діяльності організації; — безпосереднє й опосередковане хабарництво (наприклад, хабар, що пропонується або приймається через третю сторону або самою третьою стороною).

Даний документ стосується виключно тематики хабарництва. Ним окреслено вимоги та приведено настанови щодо системи управління, розробленої на підтримку організації в питаннях упередження, виявлення й реагування на випадки хабарництва, а також відповідності законам щодо протидії хабарництву й добровільних зобов'язань стосовно такої діяльності.

Зокрема даним документом не охоплено тематику шахрайства, картельних змов та інших правопорушень, які стосуються анти-трастового/конкурентного законодавства, відмивання грошей або іншої корупційної діяльності, хоча сама організація має право розширити сферу застосування системи управління, яка включала би перелічені вище порушення.

Вимоги даного документу вважаються загальними, і автори не ставили собі за мету їх застосування в усіх типах організацій або їх частинах, незалежно від їх типу, розміру та природи діяльності, або ж те, у якій сфері вони працюють (державній, приватній чи неприбутковій). Сфера застосування цих вимог залежить від факторів, що їх вказано в Статтях 4.1, 4.2 і 4.5.

ПРИМІТКА 1: Див. Статтю А.2 для ознайомлення з відповідними настановами.

ПРИМІТКА 2: Заходи, що вважаються необхідними для упередження, виявлення й мінімізації ризиків хабарництва збоку організації можуть відрізнятися від тих, що застосовуються для упередження, виявлення та реагування на випадки хабарництва всередині самої організації (збоку її персоналу чи ділових партнерів, які діють від імені організації). Див. Статтю А.8.4 для ознайомлення з відповідними настановами.

2 Нормативні посилання

Даний документ не містить жодних нормативних посилань.

3 Термінологія і визначення

У рамках даного документу вживаються наступні термінологія і визначення.

ISO та IEC ведуть термінологічні бази даних для використання у сфері стандартизації, ознайомитися з якими можна за наступними адресами в мережі Інтернет:

— Платформа для онлайн перегляду ISO: http://www.iso.org/obp

— «Електропедія» МЕК/IEC: http://www.electropedia.org/

3.1
хабарництво
пропозиція, обіцянка, передача, отримання або сприяння в отриманні неправомірної переваги будь-якої вартості (як фінансової так і не-фінансової), прямо чи опосередковано, незалежно від місця (місць) порушення застосовного права, у якості мотивації або винагороди на користь особи за певні скоєні дії або бездіяльність стосовно *виконання* (3.16) такою особою її обов'язків

Примітка 1 до запису: Вказане вище визначення вважається загальним. Значення терміну «хабарництво» - це визначення, що встановлюється антикорупційним правом, застосовним у рамках певної *організації* (3.2) та *системи управління* протидією хабарництву (3.5), яка розробляється організацією.

3.2
організація
особа або група осіб із власними функціями, обов'язками, повноваженнями та взаємовідносинами для досягнення поставлених *цілей* (3.11)
Примітка 1 до запису: Така концепція організації включає в себе, але не обмежується, фізичних осіб підприємців, компанії, корпорації, фірми, підприємства, органи влади, партнерства, благодійні об'єднання або інституції, їх частини або поєднання, з утворенням або без утворення юридичної особи, державні або приватні.

Примітка 2 до запису: Для організацій, до складу яких входить більше одного оперативного підрозділу, один або більше оперативний підрозділ може визначитися як організація.

3.3
зацікавлена сторона (бажаний термін)
«стейкхолдер»/партнер (допустимий термін)
фізична особа або *організація* (3.2), яка може впливати, підпадати під вплив або ж сприйматися як така, що підпадає під вплив певного рішення або діяльності

Примітка 1 до запису: Зацікавлена сторона може бути зовнішньою або внутрішньою стосовно організації.

3.4
вимога
зазначена потреба обов'язкового характеру

Примітка 1 до запису: Базове визначення поняття «вимоги» в стандартах системи управління ISO звучить, як «потреба або очікування, яка була зазначена, малася на увазі або вважається обов'язковою». «Вимоги, що маються на увазі» не застосовуються в контексті управління протидією хабарництву.

Примітка 2 до запису: «Вимоги, що маються на увазі» - це визначення, яке вважається індивідуальною або загальною практикою для організації та зацікавлених сторін, що несе під собою певну потребу або очікування.

Примітка 3 до запису: Вказаною вважається така вимога, яку було зазначено, наприклад, у вигляді задокументованої інформації.

3.5
система управління
набір взаємопов'язаних або взаємодіючих елементів *організації* (3.2) для формування *політики* (3.10) і *цілей* (3.11), а також *процесів* (3.15) для досягнення поставлених цілей

Примітка 1 до запису: Система управління може стосуватися одної або кількох дисциплін.

Примітка 2 до запису: Елементи системи управління включають у себе структуру організації, її функції та обов'язки, планування й діяльність.

Примітка 3 до запису: Сфера застосування системи управління може включати в себе всю організацію,

конкретні або визначені функції організації, а також окремі й визначені частини організації, одну або кілька функцій в рамках групи організацій.

3.6
вище керівництво
фізична особа або група осіб яка скеровує й контролює *організацію* (3.2) на найвищому рівні

Примітка 1 до запису: Вище керівництво має право делегувати повноваження й передавати ресурси в межах організації.

Примітка 2 до запису: Якщо сфера застосування *системи управління* (3.5) охоплює лише частину організації, тоді термін стосується тих, хто спрямовує й контролює саме таку частину організації.

Примітка 3 до запису: Організації можуть формуватися в залежності від нормативно-законодавчої бази, за якою вони працюють, а також відповідно до свого розміру, сфери діяльності, тощо. Деякі організації мають *керівний орган* (3.7) і вище керівництво, тоді як інші не розподіляють повноважень між кількома органами. Такі варіанти стосовно організації та її обов'язків можуть розглядатися під час застосування вимог Статті 5.

3.7
керівний орган
група осіб або орган, що наділена вищою відповідальністю та повноваженнями стосовно діяльності *організації* (3.2), управління нею та політикою, за якою звітує *вище керівництво* (3.6), та за якою воно підзвітне

Примітка 1 до запису: Не всі організації, і зокрема це стосується невеличких організацій, розділяють керівний орган і вище керівництво (див. 3.6, Примітка 3 до запису).

Примітка 2 до запису: Керівний орган може включати в себе, але не обмежуватися, радою директорів, комітетами ради, наглядовою раду, довіреними особами або спостерігачами.

3.8
підрозділ забезпечення нормативно-правової відповідності
особа(и), відповідальна й уповноважена на контроль за роботою *системи управління* протидією хабарництву (3.5)

3.9
ефективність
межа, до якої вдалося досягти запланованих і реалізованих результатів

3.10
політика
наміри й напрям діяльності *організації* (3.2) відповідно до формального визначення її *вищого*

керівництва (3.6) або *керівного органу* (3.7)

3.11
ціль
результат, якого планується досягти

Примітка 1 до запису: Ціль може бути стратегічною, тактичною або оперативною.

Примітка 2 до запису: Цілі можуть стосуватися різних сфер (наприклад, фінансової, продажів і маркетингу, закупівель, охорони здоров'я й безпеки або ж охорони середовища) і різних рівнів (наприклад, стратегічного, організаційного, проектного, продукту й *процесу* (3.15)).

Примітка 3 до запису: Ціль може виражатися іншим способом, наприклад, бажаним результатом, метою, оперативним критерієм, ціллю протидії хабарництву, або ж використовувати інші слова аналогічного значення.

Примітка 4 до запису: У контексті *систем управління* протидією хабарництву (3.5) цілі такої протидії встановлюються конкретною *організацією* (3.2) і відповідають *політиці* протидії хабарництву (3.10) для досягнення конкретних результатів.

3.12
ризик
ефект невизначеності для поставлених *цілей* (3.11)

Примітка 1 до запису: Ефект – це відхилення від очікуваного – позитивного або негативного значення.

Примітка 2 до запису: Невизначеність – це стан браку (навіть часткового) відповідної інформації, розуміння або знань про певну подію, її наслідки або вірогідність.

Примітка 3 до запису: Ризик часто характеризується посиланням на потенційні «події» (за визначенням Посібника ISO 73:2009, 3.5.1.3) та «наслідки» (за визначенням Посібника ISO 73:2009, 3.6.1.3) або ж поєднанням обох перелічених понять.

Примітка 4 до запису: Ризик часто визначається поєднанням наслідків події (включаючи зміни обставин), а також пов'язаною «вірогідністю» (за визначенням Посібника ISO 73:2009, 3.6.1.1) того, що така подія відбудеться.

3.13
компетентність
здатність застосовувати знання й навички для досягнення запланованих результатів

3.14
задокументована інформація
інформація, що вимагає контролю й актуалізації збоку *організації* (3.2), а також середовище, в якому міститься така інформація

Примітка 1 до запису: Задокументована інформація може бути в будь-якому форматі, середовищі і з будь-якого джерела.

Примітка 2 до запису: Задокументована інформація може посилатися на:
— *систему управління* (3.5), включаючи відповідні *процеси* (3.15);
— інформацію, створену для організації роботи (документацію);
— докази досягнутих результатів (записи).

3.15
процес
набір взаємопов'язаних та взаємодіючих видів діяльності, які перетворюють вхідні ресурси на остаточний продукт

3.16
виконання
вимірюваний результат

Примітка 1 до запису: Виконання може стосуватися кількісних або якісних результатів.

Примітка 2 до запису: Виконання може стосуватися управління діяльністю, *процесами* (3.15), продуктами (включаючи послуги), системами або *організаціями* (3.2).

3.17
«аутсорсинг»
домовленість, у рамках якої зовнішня *організація* (3.2) виконує частину діяльності або *процесів* (3.14) організації

Примітка 1 до запису: Зовнішня організація знаходиться поза межами *системи управління* (3.5), хоча функція або процес, яка віддається на «аутсорсинг», знаходиться в її межах.

Примітка 2 до запису: Базовий тест стандартів системи управління ISO містить визначення та вимоги до «аутсорсинг», які не входять до даного документу, адже постачальники послуг із «аутсорсингу» входять до визначення поняття *діловий партнер* (3.26).

3.18
моніторинг
визначення статусу системи, *процесу* (3.15) або діяльності

Примітка 1 до запису: Для визначення статусу потрібно провести перевірку, нагляд або критичне спостереження.

3.19
вимірювання
процес (3.15) встановлення значення

3.20
аудит
систематичний, незалежний і задокументований *процес* (3.15) для отримання доказів аудиту і їх об'єктивної оцінки з метою визначення ступеня виконання критеріїв аудиту

Примітка 1 до запису: Аудит може бути внутрішнім (перша сторона) або зовнішнім (друга або третя сторона), і він може бути комбінованим (тобто поєднувати дві і більше сфери діяльності).

Примітка 2 до запису: Внутрішній аудит проводиться самою *організацією* (3.2) або зовнішньою стороною від її імені.

Примітка 3 до запису: Визначення понять «Докази аудиту» й «критерії аудиту» приведено в Стандарті ISO 19011.

3.21
відповідність
виконання *вимоги* (3.4)

3.22
невідповідність
невиконання *вимоги* (3.4)

3.23
коригування
дія з усунення причин *невідповідності* (3.22) та упередження повторних невідповідностей

3.24
постійне вдосконалення
регулярна діяльність із покращення *виконання* (3.16)

3.25
персонал
директори, службовці, наймані працівники, тимчасові працівники, робітники й волонтери *організації* (3.2)

Примітка 1 до запису: Різні типи персоналу стикаються з різними рівнями *ризику* (3.12) хабарництва, і до них може бути різне ставлення протягом процедур оцінки ризику хабарництва в організації, а також управління ризиками хабарництва.

Примітка 2 до запису: Див. A.8.5 для настанов тимчасовому персоналу або робітникам.

3.26
діловий партнер
зовнішня сторона, з якою *організація* (3.2) має або планує встановити певну форму ділових відносин

Примітка 1 до запису: Ділові партнери включають у себе але не обмежуються клієнтами, замовниками, спільними підприємствами, партнерам за спільними підприємствами, партнерами консорціуму, постачальниками послуг із «аутсорсингу», виконавцями, консультантами, субпідрядниками, постачальниками, продавцями, радниками, агентами, дистриб'юторами, представниками, посередниками та інвесторами. Таке визначення широке, і його слід тлумачити відповідно до профілю
ризику (3.12) хабарництва в організації для застосування його до ділових партнерів які можуть становити обґрунтований ризик хабарництва для організації.

Примітка 2 до запису: Різні типи ділових партнерів становлять різні типи й ступені ризику хабарництва, і *організація* (3.2) матиме різні рівні потенціалу впливати на різні типи ділових партнерів. До різних типів ділових партнерів може бути різне ставлення протягом процедур оцінки ризиків хабарництва в організації та управління ризиками хабарництва.

Примітка 3 до запису: Посилання на «ділових» у даному документі може тлумачитися широко для

 визначення типів діяльності, які стосується мети існування організації.

3.27
державний службовець
особа, яка займає законодавчу, адміністративну або суддівську посаду за призначенням, виборну або успадковану, або ж будь-яка особа, що виконує державну функцію, включаючи державне агентство або державне підприємство, або ж будь-яка посадова особа чи агент державної національної або міжнародної організації, або ж кандидат на перераховані вище посади

Примітка 1 до запису: Приклади осіб, яких можна вважати державними службовцями, приведено в Статті А.21.

3.28
третя сторона
особа або орган, незалежна від *організації* (3.2)

Примітка 1 до запису: Усі *ділові партнери* (3.26) вважаються третіми сторонами, але не всі треті сторони вважаються діловими партнерами.

3.29
конфлікт інтересів
ситуація, у якій ділові, фінансові, сімейні, політичні або особисті інтереси можуть впливати на неупередженість осіб у виконанні ними своїх обов'язків у *організації* (3.2)

3.30
комплексна перевірка («due diligence»)
процес (3.15) подальшої оцінки природи та ступеня *ризику* (3.12) хабарництва для допомоги також *організаціям* (3.2) в ухваленні рішень стосовно певних правочинів, проектів, діяльності, *ділових партнерів* (3.26) і персоналу

4 Контекст організації

4.1. Розуміння організації та її контексту

Організація повинна визначати зовнішні та внутрішні питання стосовно своєї мети, та які впливають на її здатність досягати поставлених цілей системи управління протидією хабарництву. Такі питання включають у себе але не обмежуються наступними факторами:

а. розмір, структура й делеговані повноваження з ухвалення рішень організації; б. місця

й сфери, у яких працює або планує працювати організація;

в. природа, масштаби й складність діяльності та функціонування організації; г.

бізнес-модель організації;

д. юридичні особи під контролем організації, а також ті, які контролюють саму організацію; е. ділові

партнери організації;

ж. природа й ступінь взаємодії з державними службовцями;

з. застосовні статутні, нормативні, контрактні й професійні зобов'язання й обов'язки.

ПРИМІТКА: Вважається, що організація контролює іншу організацію в тому випадку, коли вона безпосередньо або опосередковано контролює управління такою організацією (див. А.13.1.3).

4.2. Розуміння потреб та очікувань зацікавлених сторін

Організація повинна визначати:

а. зацікавлені сторони (партнерів), що мають відношення до системи управління протидією хабарництву;

 б. відповідні вимоги до таких зацікавлених сторін (партнерів).

ПРИМІТКА: Протягом визначення вимог до зацікавлених сторін (партнерів) організація спроможна розрізняти обов'язкові вимоги та необов'язкові очікування або ж добровільні зобов'язання зацікавлених сторін (партнерів).

4.3. Визначення сфери застосування системи управління протидією хабарництву

Організація повинна визначити межі й застосовність системи управління протидією хабарництву для формування сфери застосування останньої.

Протягом визначення сфери застосування організація повинна зважати на наступне: а. зовнішні та внутрішні питання, вказані в 4.1;

б. вимоги, вказані в 4.2;

в. результати оцінки ризиків хабарництва, вказані в 4.5.

Сфера застосування подається у вигляді задокументованої інформації.

ПРИМІТКА: Для детальної інформації дивіться Статтю А.2.

4.4. Система управління протидією хабарництву

Організація повинна створити, документувати, реалізовувати, підтримувати та постійно переглядати, а також удосконалювати (за існування такої необхідності) систему управління протидією хабарництву, включаючи необхідні процеси та взаємодії між ними, відповідно до вимог цього документу.

Система управління протидією хабарництву повинна містити виміри, які розроблено для визначення й оцінки ризику, а також упередження, виявлення та реагування на випадки хабарництва.

ПРИМІТКА 1: Повністю усунути ризик хабарництва неможливо, і жодна система управління протидією хабарництву не зможе упередити або виявити усі типи хабарництва.

Система управління протидією хабарництву повинна бути обґрунтованою й пропорційною, зважаючи на фактори, вказані в 4.3.

ПРИМІТКА 2: Для детальної інформації дивіться Статтю А.3.

4.5. Оцінка ризику хабарництва

4.5.1. Організація зобов'язана проводити регулярну оцінку(и) ризиків хабарництва, яка повинна:

а. виявляти ризики хабарництва, які може обґрунтовано очікувати організація, зважаючи на фактори, перелічені в 4.1;

б. аналізувати, оцінювати й визначити пріоритети ризиків хабарництва;

в. проводити оцінку придатності й ефективності чинних засобів контролю організації для мінімізації оцінених ризиків хабарництва.

4.5.2. Організація зобов'язана встановити критерії оцінки ступеня ризику хабарництва, на які слід зважати в рамках політики й цілей організації.

4.5.3. Оцінка ризиків хабарництва повинна переглядатися:

а. на регулярній основі задля належної оцінки нової інформації на базі графіку й частоти, визначених організацією;

 б. у випадку значних змін структури або діяльності організації.

4.5.4. Організація зобов'язана зберігати задокументовану інформацію, яка підтверджує проведення оцінки ризиків хабарництва й використовується для розробки або вдосконалення системи управління протидією хабарництву.

ПРИМІТКА: Для детальної інформації дивіться Статтю A.4.

5. Керівництво

5.1. Керівництво та зобов'язання

5.1.1. Керівний орган

Коли в організації є керівний орган, такий орган зобов'язаний демонструвати керівництво й зобов'язання стосовно системи управління протидією хабарництву наступним чином:

а. затвердження політики протидії хабарництву організації;

б. забезпечення відповідності стратегії й політики протидії хабарництву організації;

в. отримання й перегляд інформації стосовно змісту й функціонування системи управління протидією хабарництву організації у визначені інтервали;

г. вимоги щодо виділення й призначення належних ресурсів відповідного об'єму, потрібних для ефективного функціонування системи управління протидією хабарництву організації;

д. здійснення обґрунтованого нагляду за реалізацією системи управління протидією хабарництву організації вищим керівництвом та ефективністю такої реалізації.

Перелічені вище заходи повинні виконуватися вищим керівництвом у тому випадку, коли організація не має окремого керівного органу.

5.1.2. Вище керівництво

Вище керівництво зобов'язане демонструвати керівництво й зобов'язання стосовно системи управління протидією хабарництву наступним чином:

а. забезпечення створення, реалізації, підтримки й перегляду системи управління протидією хабарництву, включаючи політику й цілі, для належного реагування на ризики хабарництва для організації;

б. забезпечення інтеграції вимог системи управління протидією хабарництву до процесів організації;

в. розгортання належних і відповідних ресурсів для ефективної роботи системи управління протидією хабарництву;

г. внутрішня й зовнішня комунікація стосовно політики протидії хабарництву;

д. внутрішня комунікація стосовно важливості ефективного управління протидією хабарництву й відповідності вимогам системи управління протидією хабарництву;

е. забезпечення належної розробки системи управління протидією хабарництву для досягнення поставлених цілей;

ж. спрямування й підтримка персоналу для забезпечення ефективності роботи системи управління протидією хабарництву;

з. просування належної культури боротьби з хабарництвом в організації; и.

просування практики постійного вдосконалення;

к. підтримка інших відповідних управлінських функцій для демонстрації керівної позиції в питаннях упередження й виявлення хабарництва, адже це стосується їх сфер відповідальності;

л. заохочення використання процедур звітності для випадків вірогідного й реального хабарництва (див. 8.9);

м. убезпечення персоналу від переслідування, дискримінації, або дисциплінарних покарань (див. 7.2.2.1 г)) за достовірні надані звіти або такі повідомлення, що базуються на обґрунтованих підозрах або вірогідності політики протидії хабарництву організації, або ж відмови брати участь у спробі хабарництва, навіть якщо така відмова може призвести до втрати ділових інтересів організації (окрім тих випадків, коли фізична особа бере особисту участь у правопорушеннях);

н. регулярне звітування перед керівним органом (якщо такий є) про наповнення й функціонування системи управління протидією хабарництву, а також підозри щодо серйозних або систематичних

випадків хабарництва.

ПРИМІТКА: Для детальної інформації дивіться Статтю А.5.

5.2. Політика протидії хабарництву

Вище керівництво зобов'язане створити, підтримувати й переглядати політику протидії хабарництву, яка:

а. забороняє хабарництво;

б. вимагає відповідності вимогам законодавства у сфері протидії хабарництву, яке застосовується в організації;

в. відповідає загальній меті організації;

г. надає рамки для створення, перегляду й досягнення цілей боротьби з хабарництвом;

д. включає в себе зобов'язання задовольнити вимоги системи управління протидією хабарництву;

е. заохочує обґрунтовані підозри або ж такі, що базуються на вагомих підставах вважати, без остраху переслідувань;

ж. включає в себе зобов'язання щодо постійного вдосконалення системи управління протидією хабарництву;

з. пояснює повноваження й незалежність Підрозділу забезпечення нормативно-правової відповідності;

и. пояснює наслідки невиконання політики протидії хабарництву.

Політика протидії хабарництву повинна:

— бути доступною у вигляді задокументованої інформації;

— подаватися відповідними мовами для організації й ділових партнерів, які становлять ступінь ризику хабарництва, вищий за «низький»;

— бути доступною для відповідних зацікавлених сторін (партнерів) у разі такої необхідності.

5.3. Організаційні функції, відповідальність та повноваження 5.3.1.

Функції та відповідальність

Вище керівництво повинно нести загальну відповідальність за реалізацію й відповідність системи управління протидією хабарництву, як це описується в 5.1.2.

Вище керівництво повинно забезпечити розподіл і комунікацію відповідальності й повноважень для відповідних функцій, а також їх комунікацію по всім рівням організації.

Керівники кожного рівня повинні нести відповідальність за вимоги застосування вимог системи управління протидією хабарництву та відповідність таким вимогам у їх департаментах чи підрозділах.

Керівний орган (якщо такий є), вище керівництво та весь інший персонал повинен нести відповідальність за розуміння, відповідність та застосування вимог системи управління протидією хабарництву, відповідно до своїх функцій в організації.

5.3.2. Підрозділ забезпечення нормативно-правової відповідності

Вище керівництво повинно передати Підрозділу забезпечення нормативно-правової відповідності відповідальність і повноваження для:

а. нагляду за розробкою й реалізацією організацією системи управління протидією хабарництву;

б. надання дорадчої допомоги й настанов персоналу щодо системи управління протидією хабарництву та питань, які стосуються проблеми хабарництва;

в. забезпечення відповідності системи управління протидією хабарництву вимогам цього документу;

г. звітування про виконання системи управління протидією хабарництву перед керівним органом (якщо такий є) і вищим керівництвом, а також іншими підрозділами із забезпечення

відповідності в разі виникнення такої потреби.

Підрозділ забезпечення нормативно-правової відповідності повинен бути належним чином забезпечений ресурсами й персоналом відповідної компетенції, статусу, повноважень і незалежності.

Підрозділ забезпечення нормативно-правової відповідності повинен мати безпосередній і оперативний доступ до керівного органу (якщо такий є) і вищого керівництва на випадок потреби у вирішенні проблем або питань стосовно випадків хабарництва чи системи управління протидією хабарництву.

Вище керівництво спроможне передати деякі або всі функції Підрозділу забезпечення нормативно-правової відповідності зовнішнім для організації особам. У такому випадку вище керівництво повинно забезпечити, щоб певний персонал ніс відповідальність та мав повноваження щодо таких переданих на зовнішнє виконання функцій.

ПРИМІТКА: Для детальної інформації дивіться Статтю А.6.

5.3.3. Делегування ухвалення рішень

У тому випадку, коли вище керівництво делегує персоналу повноваження щодо ухвалення рішень, стосовно яких існує ризик хабарництва зі ступенем вище «низького», організація повинна створити й підтримувати процес ухвалення рішень або набір елементів управління, який вимагає, щоб процес ухвалення рішень та рівень повноважень особи (осіб), яка такі рішення ухвалює, були належного рівня, а також позбавленими будь-яких реальних або потенційних конфліктів інтересів. Вище керівництво повинно забезпечити, щоб усі процеси регулярно переглядалися в рамках своєї функції й відповідальності з реалізації та відповідності системи управління протидією хабарництву, як це вказано в 5.3.1.

ПРИМІТКА: Делегування ухвалення рішень не звільняє вище керівництво або керівний орган (якщо такий є) від їх обов'язків, як це описано в 5.1.1, 5.1.2 і 5.3.1, і не обов'язково перекладає потенційну правову відповідальність на персонал, якому делегуються такі повноваження.

МІЖНАРОДНИЙ СТАНДАРТ ISO 37001:2016(E) 6. Планування

6.1. Діяльність стосовно ризиків та можливостей

Протягом планування для роботи системи управління протидією хабарництву, організація повинна розглянути питання, на які посилаються в 4.1, а також вимоги, на які посилаються в 4.2, ризики, виявлені в 4.5, та можливості вдосконалення для:

а. належного забезпечення досягнення системою управління протидією хабарництву її цілей;

б. упередження або мінімізації небажаного ефекту для політики й цілей протидії хабарництву;

в. моніторингу ефективності системи управління протидією хабарництву; г.

досягнення постійного вдосконалення.

Організація повинна планувати наступне:

− заходи з розгляду відповідних ризиків хабарництва та можливостей для вдосконалення; − яким чином:

- − інтегрувати й реалізувати такі заходи у свої процеси системи управління протидією хабарництву;
- − оцінити ефективність таких заходів.

6.2. Цілі протидії хабарництву та планування з їх досягнення

Організація повинна встановити цілі системи управління протидією хабарництву для відповідних підрозділів і рівнів.

Цілі системи управління протидією хабарництву повинні:

а. бути узгодженими з політикою протидії хабарництву;

б. бути вимірюваними (якщо це практично можливо);

в. зважати на застосовні фактори, які вказано в 4.1, вимоги, на які посилаються в 4.2, та ризики

хабарництва, визначені в 4.5;

г. бути досяжними;

д. підлягати моніторингу;

е. підлягати комунікації відповідно до 7.4;

ж. поновлюватися за необхідністю.

Організація повинна зберігати задокументовану інформацію про цілі системи управління протидією хабарництву.

Протягом планування досягнення цілей системи управління протидією хабарництву організація повинна визначити:

— що буде зроблено;

— які знадобляться ресурси;

— хто нестиме відповідальність;

— коли буде досягнуто цілей;

— які результати будуть оцінюватися та звітуватися;

— хто накладатиме штрафи або санкції.

МІЖНАРОДНИЙ СТАНДАРТ ISO 37001:2016(E) 7. Підтримка

7.1. Ресурси

Організація повинна визначити й надати ресурси, потрібні для створення, реалізації, обслуговування й постійного вдосконалення системи управління протидією хабарництву.

ПРИМІТКА: Для детальної інформації дивіться Статтю A.7.

7.2. Компетентність

7.2.1. Загальні положення

Організація повинна:

а. визначити необхідну компетенцію особи (осіб), які працюють під її контролем, що впливає на виконання діяльності з протидії хабарництву;

б. забезпечити, щоб компетентність таких осіб базувалася на відповідній освіті, підготовці або досвіді;

в. у разі необхідності – вжити заходів для отримання й підтримки необхідної компетенції, а також оцінки ефективності вжитих заходів;

г. зберігати відповідну задокументовану інформацію в якості доказів компетентності.

ПРИМІТКА: Застосовні заходи можуть включати, наприклад, проведення тренінгів, «коучингу» або перепризначення персоналу чи ділових партнерів, або ж найм чи підписання контракту на аналогічні види діяльності.

7.2.2. Процес найму

7.2.2.1. Організація повинна реалізовувати процедури стосовно всього персоналу для забезпечення того, щоб:

а. умови найму вимагали від персоналу відповідності положенням політики протидії хабарництву та системи управління протидією хабарництву, а також давали організації право дисциплінувати персонал у випадку невідповідності;

б. у рамках обґрунтованого періоду заступання на роботу персонал отримав копію або ж доступ до документу політики протидії хабарництву та пройшов підготовку стосовно такої політики;

в. організація мала процедури, які б дозволяли їй вживати відповідних дисциплінарних заходів стосовно персоналу, який порушує політику протидії хабарництву або ж вимоги системи

управління протидією хабарництву;

г. персонал на став жертвою переслідувань, дискримінації або дисциплінарних покарань (наприклад, від погроз, ізоляції, пониження в посаді, перешкоджання в підвищенні, переведення, звільнення, агресивної поведінки, «віктимізації» чи інших форм переслідування) за:

1) відмову від участі в будь-якій діяльності, ступінь ризику хабарництва якої обґрунтовано оцінюється як такий, що перевищує «низький», і який не було мінімізовано організацією; або

2) повідомлення чи обґрунтовані звіти або ж такі, що ґрунтуються на обґрунтованих підозрах, щодо спроби, реального або підозрюваного факту хабарництва або порушення політики протидії хабарництву чи вимог системи управління протидією хабарництву (окрім тих випадків, коли фізична особа бере особисту участь у правопорушеннях).

7.2.2.2. Стосовно всіх посад, ступінь ризику яких вищий за «низький», що підтверджується оцінкою ризиків хабарництва (див. 4.5), а також для забезпечення роботи Підрозділу забезпечення нормативно-правової відповідності, організація повинна реалізувати процедури, які забезпечують:

а. виконання комплексної перевірки «due diligence» (див. 8.2) для фізичних осіб перед їх працевлаштуванням, а також для персоналу – перед їх переведенням або підвищенням у рамках організації для забезпечення, наскільки це розумно, що персонал слід найняти або перепризначити, а також, що є обґрунтовані підстави вважати, що працівники відповідають вимогам політики протидії хабарництву та системи управління протидією хабарництву;

б. регулярний перегляд службових премій, показників ефективності й інших мотиваційних елементів оплати праці для перевірки надійності встановлених обґрунтованих гарантій запобігання заохочень до хабарництва;

в. що такий персонал, вище керівництво та керівний орган (якщо такий є) подавали декларацію, яка б підтверджувала їх відповідність вимогам політики протидії хабарництву з обґрунтованою регулярністю, яка була би пропорційною виявленому ризику хабарництва.

ПРИМІТКА 1: Декларація відповідності вимогам протидії хабарництву може подаватися окремо або в якості складової ширшого процесу декларування відповідності.

ПРИМІТКА 2: Для детальної інформації дивіться Статтю А.8.

7.3. Інформування та навчання

Організація повинна забезпечити адекватне й відповідне інформування й навчання персоналу щодо питань протидії хабарництву. Таке навчання повинно охоплювати наступні питання (у разі необхідності), зважаючи на результати оцінки ризиків хабарництва (див. 4.5):

а. політика протидії хабарництву, процедури та система управління протидією хабарництву організації, а також обов'язковість відповідності;

б. ризик хабарництва та шкоди від нього для персоналу й організації;

в. обставини, за яких може траплятися хабарництво стосовно обов'язків персоналу, а також яким чином можна виявити такі обставини;

г. яким чином розпізнати та реагувати на підбурювання або спроби дати хабара;

д. яким чином персонал може допомогти із запобіганням або уникненням хабарництва, а також яким чином можна розпізнати ключові індикатори ризику хабарництва;

е. внесок персоналу до ефективності системи управління протидією хабарництву, включаючи переваги від вдосконалених заходів протидії хабарництву та звітування про підозри щодо хабарництва;

ж. висновки й потенційні наслідки невідповідності вимогам системи управління протидією хабарництву;

з. яким чином і кому персонал повинен повідомляти про будь-які проблемні питання (див. 8.9);

и. інформація про доступні тренінги й ресурси.

Персонал необхідно регулярно інформувати та готувати з питань протидії хабарництву (із періодичністю, яку планує організація) відповідно до функцій працівників, ризиків хабарництва, з

якими вони матимуть справу, та будь-які змінні умови. У разі необхідності процедури інформування й навчання потрібно переглядати й поновлювати для відображення нової актуальної інформації.

Зважаючи на виявлені ризики хабарництва (див. 4.5), організація повинна також займатися

реалізацією процедур інформування й навчання з питань протидії хабарництву для ділових партнерів, які виступають від імені такої організації або в її інтересах, і які можуть становити для організації ризик зі ступенем вище «низького». Такі процедури повинні виявляти ділових партнерів, щодо яких необхідно вжити відповідних заходів з інформування й навчання, наповнення та інструментарію тренінгів та навчання.

Організація повинна зберігати задокументовану інформацію з процедур навчання й підготовки, змісту навчання й підготовки, а також часу її проведення, і для кого вона проводилася.

ПРИМІТКА 1: Вимоги до інформування й навчання ділових партнерів можуть передаватися в рамках контрактних або аналогічних вимог, а також реалізовуватися організацією, діловим партнером або будь якими іншими сторонами, призначеними з цією метою.

ПРИМІТКА 2: Для детальної інформації дивіться Статтю A.9.

7.4. Комунікація

7.4.1. Організація повинна визначити внутрішні й зовнішні канали комунікації, які стосуються системи управління протидією хабарництву, включаючи наступні питання:

а. тематика комунікації;

б. час комунікації;

в. особи, з якими встановлюється комунікація;

г. спосіб комунікації;

д. особи, які будуть займатися комунікацією;

е. мови комунікації.

7.4.2. Політика протидії хабарництву повинна бути доступною для всього персоналу організації та її ділових партнерів, передаватися безпосередньо персоналу та діловим партнерам, які становлять ризик хабарництва зі ступенем вище «низького», а також публікуватися через внутрішні й зовнішні комунікаційні канали в разі такої необхідності.

7.5. Задокументована інформація

7.5.1. Загальні положення

Система управління протидією хабарництву організації повинна включати в себе наступне: а.

задокументовану інформацію, яка вимагається цим документом;

б. задокументовану інформацію, яка визначається організацією в якості необхідної для ефективної роботи системи управління протидією хабарництву.

ПРИМІТКА 1: Об'єми задокументованої інформації для системи управління протидією хабарництву можуть відрізнятися для різних організацій, зважаючи на:

— розмір організації, тип її діяльності, процеси, продукти й послуги;

— складність процесів та їх взаємодії;

— компетентність персоналу.

ПРИМІТКА 2: Задокументована інформація може зберігатися окремо, як частина системи управління протидією хабарництву або ж інших систем управління (наприклад, системи відповідності, фінансової чи комерційної системи, системи аудиту, тощо).

ПРИМІТКА 3: Для детальної інформації дивіться Статтю A.17.

 7.5.2. Створення й поновлення

Протягом створення й поновлення задокументованої інформації організація повинна забезпечити належні:

а. ідентифікацію й опис (наприклад, назва, дата, автор або номер посилання);

б. формат (наприклад, мова, версія програмного забезпечення, графіка) і носій (наприклад, паперовий або електронний);

в. огляд і затвердження придатності й актуальності.

7.5.3. Контроль задокументованої інформації

Задокументована інформація, яка вимагається системою управління протидією хабарництву та цим документом, повинна контролюватися для забезпечення:

а. доступності й придатності до використання, коли й де вона потрібна;

б. належного захисту (наприклад, від порушення умов конфіденційності, неналежного використання або втрати цілісності).

Для контролю задокументованої інформації організація повинна зважати на наступні заходи, якщо вони потрібні:

— розповсюдження, доступ, отримання й використання;

— зберігання й забезпечення збереження, включаючи збереження розбірливості; —

контроль змін (наприклад, контроль версії);

— архівування й утилізація.

Задокументована інформація зовнішнього походження, яка визнається організацією необхідною для планування й роботи системи управління протидією хабарництву, повинна за існування такої необхідності ідентифікуватися й контролюватися.

ПРИМІТКА: Під «доступом» може матися на увазі рішення стосовно надання дозволу лише на перегляд задокументованої інформації або ж дозвіл і повноваження на перегляд і зміни задокументованої інформації.

8. Функціонування

8.1. Оперативне планування й контроль

Організація повинна планувати, реалізовувати, переглядати й контролювати процеси, необхідні для забезпечення виконання вимог системи управління протидією хабарництву та реалізації заходів, визначених у 6.1, шляхом:

а. встановлення критеріїв для процесів;

б. здійснення контролю процесів відповідно до встановлених критеріїв;

в. ведення задокументованої інформації для впевненості в тому, що процеси виконуються відповідно до плану.

Вказані вище процеси повинні включати в себе певні засоби контролю, на які посилаються в Статтях із 8.2 по 8.10.

Організація повинна контролювати заплановані зміни та переглядати наслідки незапланованих змін, вживаючи заходів для мінімізації будь-якого негативного впливу в разі такої потреби.

Організація повинна забезпечити контроль процесів, які передаються на «аутсорсинг».

ПРИМІТКА: Основний текст стандартів щодо систем управління ISO містить вимоги до «аутсорсингу», які не використовуються в рамках даного документу, адже постачальники таких послуг включаються у визначення поняття «ділових партнерів».

8.2. Комплексна перевірка «due diligence»

У разі, якщо оцінка ризиків хабарництва, проведена відповідно до вимог 4.5, вказує на існування ризику зі ступенем вище «низького» стосовно:

а. певних категорій правочинів, проектів або діяльності;

б. запланованих або чинних відносин із певними категоріями ділових партнерів; або в.

певних категорій персоналу на певних посадах (див. 7.2.2.2);

організація повинна оцінити природу й масштаби ризику хабарництва стосовно певних категорій правочинів, проектів або діяльності, ділових партнерів і персоналу, які підпадають під такі категорії. Така оцінка повинна включати в себе будь-які елементи комплексної перевірки «due diligence», що вважаються необхідними для отримання достатнього об'єму інформації для оцінки ризику хабарництва. Комплексна перевірка «due diligence» повинна регулярно поновлюватися для того, щоб зважати на зміни й появу нової інформації.

ПРИМІТКА 1: Організація спроможна прийти до висновку, що проводити комплексну перевірку «due diligence» для певних категорій персоналу й ділових партнерів непотрібно, вважати її необґрунтованою або диспропорційною.

ПРИМІТКА 2: Фактори, перелічені в пунктах а), б) і в) вище, не вважаються вичерпними.

ПРИМІТКА 3: Для детальної інформації дивіться Статтю А.10.

8.3. Фінансовий контроль

Організація повинна здійснювати фінансовий контроль для управління ризиком хабарництва.

ПРИМІТКА: Для детальної інформації дивіться Статтю А.11.

8.4. Не-фінансовий контроль

Організація повинна здійснювати не-фінансовий контроль для управління ризиком хабарництва в таких сферах, як закупівлі, експлуатація, продажі, комерція, кадрові ресурси, правова й нормативна діяльність.

ПРИМІТКА 1: Будь-який конкретний правочин, діяльність або відносини може підпадати під фінансовий і не-фінансовий контроль.

ПРИМІТКА 2: Для детальної інформації дивіться Статтю А.12.

8.5. Здійснення контролю протидією хабарництву підконтрольними організаціями й діловими партнерами

8.5.1. Організація повинна здійснювати процедури, які вимагають, щоб усі інші підконтрольні їй організації:

а. реалізовували систему управління протидією хабарництву організації; або б.

реалізовували власні заходи з контролю протидією хабарництву,

щоразу й лише в тій мірі, яка вважається обґрунтованою й пропорційною ризикам хабарництва, з якими стикаються підконтрольні організації, зважаючи на оцінку ризику хабарництва, проведену відповідно до 4.5.

ПРИМІТКА: Вважається, що організація контролює іншу організацію, коли вона прямо або опосередковано контролює управління нею (див. А.13.1.3).

8.5.2. Стосовно ділових партнерів, які не контролюються організацією, і для яких проведена оцінка ризиків хабарництва (див. 4.5) або комплексна перевірка «due diligence» (див. 8.2) виявила ризик хабарництва зі ступенем вище «низького», а також для яких застосування засобів контролю могло б допомогти мінімізувати відповідний ризик хабарництва, організація повинна реалізовувати процедури наступним чином:

а. організація повинна визначити, чи діловий партнер має функціонуючу систему контролю для управління відповідним ризиком хабарництва;

б. якщо діловий партнер не має функціонуючої системи контролю для управління відповідним ризиком хабарництва або ж неможливо перевірити її існування:

1) за існування практичної можливості, організація повинна вимагати від ділового партнера реалізації контролю протидії хабарництву стосовно відповідного правочину, проекту, діяльності; або

2) за відсутності практичної можливості вимагати від ділового партнера реалізації контролю протидії хабарництву, на такий фактор необхідно зважати протягом оцінки ризику хабарництва щодо такого ділового партнера (див. 4.5 і 8.2), а також на спосіб, у який організація управляє такими ризиками (див. 8.3, 8.4 і 8.5).

ПРИМІТКА: Для детальної інформації дивіться Статтю A.13.

8.6. Зобов'язання щодо протидії хабарництву

У випадку з діловими партнерами, які становлять ризик хабарництва зі ступенем вище «низького», організація зобов'язана реалізувати процедури, які за існування практичної необхідності вимагають наступне:

a. ділові партнери беруть на себе зобов'язання щодо запобігання хабарництву самостійно, від імені або в інтересах ділових партнерів, які пов'язані з відповідним правочином, проектом, діяльністю або відносинами;

б. організація може припинити відносини з діловими партнерами в тому випадку, якщо вони скоїли акт хабарництва самостійно, від імені або в інтересах ділових партнерів, які пов'язані з відповідним правочином, проектом, діяльністю або відносинами.

За відсутності практичної можливості виконати вимоги пунктів а) або б) вище, на такий фактор необхідно зважати протягом оцінки ризику хабарництва щодо такого ділового партнера (див. 4.5 і 8.2), а також на спосіб, у який організація управляє такими ризиками (див. 8.3, 8.4 і 8.5).

ПРИМІТКА: Для детальної інформації дивіться Статтю A.14.

8.7. Подарунки, прояви гостинності, пожертви та аналогічні внески

Організація повинна здійснювати процедури, призначені для запобігання пропонуванню, даруванню або прийманню подарунків, проявів гостинності, пожертв та аналогічних внесків, коли їх пропонування, дарування або приймання вважається або може вважатися хабаром.

ПРИМІТКА: Для детальної інформації дивіться Статтю A.15.

8.8. Управління у випадку невідповідності контролю протидії хабарництву

У випадку виявлення протягом комплексної перевірки «due diligence» (див. 8.2) щодо певного правочину, проекту, діяльності або відносин із діловим партнером ризиків хабарництва, які не можуть управлятися чинними засобами контролю протидією хабарництву, і якщо організація неспроможна або не бажає здійснювати додаткових або посилених засобів контролю протидією хабарництву чи вживати інших необхідних заходів (як наприклад, зміна природи правочину, проекту, діяльності або відносин), які б дозволили організації управляти

 відповідними ризиками хабарництва,

організація повинна:

a. у випадку з чинним правочином, проектом, діяльністю або відносинами – вжити заходів відповідно до ризиків хабарництва й природи правочину, проекту, діяльності або відносин для його припинення, відміни, призупинення або виходу з нього за першої ж можливості;

б. у випадку з пропозицією нового правочину, проекту, діяльності або відносин – відкласти або відмовитися приймати таку пропозицію.

8.9. Тривожні сигнали

Організація зобов'язана здійснювати процедури, які:

a. заохочують і дозволяють фізичним особам повідомляти, за існування належного обґрунтування або ж бази обґрунтовано вважати про факт спроби, підозри або реального випадку хабарництва чи будь-якого іншого порушення або недоліку в системі управління протидією хабарництву,

Підрозділу забезпечення нормативно-правової відповідності або відповідному персоналу (безпосередньо або через відповідну третю сторону);

б. за виключенням випадків, передбачених триваючим розслідуванням, вимагають, щоб організація ставилася до таких повідомлень, як до конфіденційної документації задля захисту особистості особи, яка повідомляє, а також інших залучених або згаданих у повідомленні осіб;

в. дозволяють анонімне звітування;

г. забороняють переслідування й захищають осіб, які повідомляють про порушення, від переслідування після того, як вони, за існування належного обґрунтування або ж бази обґрунтування, повідомили чи відзвітували про факт спроби, підозри або реального випадку хабарництва чи будь-якого іншого порушення політики протидії хабарництву чи вимог системи управління протидією хабарництву;

д. дозволяють персоналу отримувати поради відповідних осіб щодо можливих подальших дій у випадку підозри або реальної ситуації стосовно хабарництва.

Організація повинна забезпечити інформування всього персоналу про процедури звітування й повідомлення та можливість їх використання, а також про права й захист персоналу протягом використання таких процедур.

ПРИМІТКА 1: Такі процедури можуть бути аналогічними або частиною процедур, що використовуються для звітності й повідомлення про інші важливі питання (наприклад, питання безпеки, зловживання, протиправні дії та інші серйозні ризики).

ПРИМІТКА 2: Організація може скористатися послугами ділового партнера для управління системою звітування й повідомлення від свого імені.

ПРИМІТКА 3: У деяких юрисдикціях вимоги пунктів б) і в) вище забороняються законом. У таких випадках організація фіксує свою неспроможність їх виконати.

8.10. Розслідування та вирішення проблем хабарництва

Організація повинна здійснювати процедури, які:

а. вимагають оцінки і за необхідності – проведення розслідування будь-якого факту хабарництва або порушення політики протидії хабарництву чи вимог системи управління протидією хабарництву, про який повідомляють, який виявляють, або щодо якого існують обґрунтовані підозри;

б. вимагають належних заходів у випадку виявлення слідством будь-яких фактів хабарництва або порушення політики протидії хабарництву чи вимог системи управління протидією хабарництву;

 в. розширюють права й можливості дознавачів;

г. вимагають від відповідного персоналу співпраці зі слідством;

д. вимагають звітування про статус і результати розслідування перед Підрозділом забезпечення нормативно-правової відповідності та іншими підрозділами із забезпечення відповідності в разі такої потреби;

е. вимагають, щоб розслідування велося конфіденційно, а його результати також були конфіденційними.

Розслідування повинно проводитися персоналом, а про його хід і результати необхідно повідомляти персоналу, який не вважається частиною підрозділів і не виконує функцій, що вважаються об'єктом розслідування. Організація має можливість призначити ділового партнера відповідальним за проведення розслідування й звітування про його результати перед персоналом, який не вважається частиною підрозділів і не виконує функцій, що вважаються об'єктом розслідування.

ПРИМІТКА 1: Для детальної інформації дивіться Статтю A.18.

ПРИМІТКА 2: У деяких юрисдикціях вимоги пункту е) вище забороняються законом. У таких випадках організація фіксує свою неспроможність їх виконати.

9. Оцінка виконання

9.1. Моніторинг, вимірювання, аналіз та оцінка

Організація повинна визначити:

а. що має стати об'єктом моніторингу й вимірювання;

б. хто буде відповідальним за проведення моніторингу;

в. методи моніторингу, вимірювання, аналізу й оцінки, залежно від обставин, для забезпечення обґрунтованих результатів;

г. час проведення моніторингу й вимірювання;

д. час проведення аналізу й оцінки результатів моніторингу й вимірювання; е. кому

і як звітувати про таку інформацію.

Організація повинна зберігати відповідну задокументовану інформацію в якості доказової бази використаних методів і отриманих результатів.

Організація повинна проводити оцінку виконання, ефективності й результативності роботи системи управління протидією хабарництву.

ПРИМІТКА: Для детальної інформації дивіться Статтю А.19.

9.2. Внутрішній аудит

9.2.1. Організація повинна проводити регулярні внутрішні аудити для отримання інформації з приводу того, чи система управління протидією хабарництву:

а. відповідає:

1) власним вимогам організації до системи управління протидією хабарництву; 2)

вимогам даного документу;

б. ефективно використовується й обслуговується.

ПРИМІТКА 1: Настанови з аудиту систем управління приведено в Стандарті ISO 19011.

ПРИМІТКА 2: Сфера застосування й масштаби внутрішнього аудиту організації можуть відрізнятися залежно від таких факторів, як розмір, структура, зрілість та місце розташування організації.

9.2.2. Організація повинна:

а. планувати, створювати, реалізовувати й обслуговувати програму(и) аудиту, що включає в себе частоту, методи, відповідальність, вимоги до планування й звітування, які зважатимуть на важливість задіяних процесів та результати попередніх аудитів;

б. визначати критерії аудиту й склад кожного аудиту;

в. відбирати компетентних аудиторів і проводити аудити для забезпечення об'єктивності й неупередженості процесу аудиту;

г. забезпечувати звітування про результати аудитів перед відповідними керівниками, Підрозділом забезпечення нормативно-правової відповідності, вищим керівництвом та – за існування такої потреби – керівним органом (якщо такий є);

д. зберігати задокументовану інформацію в якості доказів реалізації програми й результатів аудиту.

9.2.3. Такі аудити повинні бути обґрунтованими, пропорційними й базуватися на ризиках. Вони також повинні включати в себе процеси внутрішнього аудиту й інші процедури, які аналізують процедури, засоби контролю й системи стосовно:

а. хабарництва або підозри щодо хабарництва;

б. порушень політики протидії хабарництву або вимог системи управління протидією хабарництву;

в. неспроможності ділових партнерів забезпечити відповідність застосовним вимогам протидії хабарництву організації;

г. недоліків або варіантів удосконалення системи управління протидією хабарництву.

9.2.4. Для забезпечення об'єктивності й неупередженості таких програм аудиту організація повинна забезпечити проведення аудитів одною з наступних сторін:

а. незалежним підрозділом або персоналом, створеним або призначеним для виконання такого процесу;

б. Підрозділом забезпечення нормативно-правової відповідності (за виключенням випадків, коли сфера застосування аудиту включає в себе оцінку самої системи управління протидією хабарництву або аналогічну роботу, за виконання якої несе відповідальність Підрозділ забезпечення нормативно-правової відповідності);

в. відповідною особою з іншого департаменту або підрозділу окрім того, який вважається об'єктом аудиту;

г. відповідною третьою стороною;

д. групою сторін у будь-якому поєднанні пунктів з а) по г).

Організація повинна забезпечити, щоб жоден аудитор не проводив аудиту власної робочої сфери.

ПРИМІТКА: Для детальної інформації дивіться Статтю А.16.

9.3. Аналіз збоку керівництва

9.3.1. Аналіз збоку вищого керівництва

Вище керівництво повинно проводити плановий аналіз системи управління протидією хабарництву організації для забезпечення її постійної придатності, адекватності й

 ефективності.

Аналіз збоку вищого керівництво повинен зважати на наступне:

а. статус заходів попередніх аналізів збоку керівництва;

б. зміни зовнішньої і внутрішньої проблематики, які стосуються системи управління протидією хабарництву;

в. інформацію про роботу (виконання) системи управління протидією хабарництву, включаючи чинні тенденції щодо:

1) невідповідностей і коригування;

2) результати моніторингу й вимірювання;

3) результати аудиту;

4) звіти про факти хабарництва;

5) розслідування;

6) природу й масштаби ризиків хабарництва, з якими стикається організація; г.

ефективність заходів, вжитих для мінімізації ризиків хабарництва;

д. можливості постійного вдосконалення системи управління протидією хабарництву відповідно до 10.2.

Результати аналізу збоку вищого керівництва повинні включати в себе рішення, ухвалені стосовно постійного вдосконалення та будь-які потреби в змінах до системи управління протидією хабарництву.

Стислий огляд результатів аналізу збоку вищого керівництва повинен повідомлятися керівному органому (якщо такий є).

Організація повинна зберігати задокументовану інформацію в якості доказів результатів аналізів збоку вищого керівництва.

9.3.2. Аналіз збоку керівного органу

Керівний орган (якщо такий є) зобов'язаний проводити регулярний аналіз системи управління

протидією хабарництву на основі інформації, наданої вищим керівництвом і Підрозділом забезпечення нормативно-правової відповідності, а також будь-якої іншої інформації, щодо якої надсилає або отримує запит керівний орган.

Організація повинна зберігати стислий огляд задокументованої інформації в якості доказу результату аналізів збоку керівного органу.

9.4 Аналіз збоку Підрозділу забезпечення нормативно-правової відповідності

Підрозділ забезпечення нормативно-правової відповідності повинен на постійній основі проводити оцінку системи управління протидією хабарництву стосовно:

а. її адекватності для ефективного управління ризиками хабарництва, з якими стикається організація;

б. ефективності її реалізації.

Підрозділ забезпечення нормативно-правової відповідності повинен звітувати із визначеною регулярністю а також на спеціальній основі в разі такої необхідності перед керівним органом (якщо такий є) і вищим керівництвом або ж відповідним комітетом керівного органу чи вищого керівництва про адекватність та реалізацію системи управління протидією хабарництву, що включає в себе результати відповідних розслідувань і аудитів.

ПРИМІТКА 1: Частота таких звітів залежить від вимог організації, але їх рекомендується проводити

 принаймні раз на рік.

ПРИМІТКА 2: Організація має можливість використати ділового партнера для підтримки в проведенні аналізу допоки повідомлення ділового партнера належним чином доводяться до відома Підрозділу забезпечення нормативно-правової відповідності, вищого керівництва та – у разі такої необхідності – керівного органу (якщо такий є).

10. Удосконалення

10.1. Невідповідність та коригування

У випадку невідповідностей організація повинна:

а. оперативно реагувати на невідповідність та залежно від обставин:

1) вживати заходів для її контролю й коригування;

2) працювати з наслідками;

б. оцінювати потребу в заходах із усунення причини (причин) невідповідності задля того, щоб попередити повторення невідповідності в майбутньому або в іншому місці шляхом:

1) проведення аналізу невідповідності;

2) визначення причин невідповідності;

3) визначення факту існування аналогічних невідповідностей або ж їх потенційного існування;

в. вживати будь-яких необхідних заходів;

г. проводити аналіз будь-яких вжитих заходів із коригування;

д. вносити зміни до системи управління протидією хабарництву в разі такої потреби. Заходи з коригування повинні відповідати ефекту виявлених невідповідностей.

Організація повинна зберігати задокументовану інформацію в якості доказів: —

природи невідповідностей і будь-яких подальших вжитих заходів;

— результатів будь-яких заходів із коригування.

ПРИМІТКА: Для детальної інформації дивіться Статтю А.20.

10.2. Постійне вдосконалення

Організація повинна займатися постійним удосконаленням придатності, адекватності й ефективності системи управління протидією хабарництву.

ПРИМІТКА: Для детальної інформації дивіться Статтю А.20.

Додаток А
(інформативний)

Посібник із використання даного документу

А.1. Загальна інформація

Настанови, приведені в даному Додатку, слід розглядати виключно в якості ілюстрацій. Мета Додатку полягає в тому, щоб вказати на певні сфери та певний тип заходів, яких спроможна вжити організація протягом експлуатації своєї системи управління протидією хабарництву. Автори не ставили собі за мету зробити Додаток комплексним або нормативним, а від організації не вимагається реалізовувати наступні кроки для того, щоб отримати систему управління протидією хабарництву, що відповідає вимогам даного документу. Кроки, що їх робить організація, повинні бути обґрунтованими й пропорційними стосовно природи й масштабів ризиків хабарництва, з якими має справу така організація (див. 4.5 та фактори, перелічені в пунктах 4.1 і 4.2).

Подальші настанови з належної практики управління протидією хабарництву можна знайти в публікаціях, що їх приведено в Бібліографії.

А.2. Сфера застосування системи управління протидією хабарництву А.2.1.

Автономна або інтегрована система управління протидією хабарництву

Організація може обирати між реалізацією цієї системи управління протидією хабарництву в якості автономної системи або інтегрованої частини загальної системи управління відповідністю (у даному випадку організація може звернутися до Стандарту ISO 19600 для отримання детальної інформації). Організація також вільна обирати реалізацію такої системи управління протидією хабарництву паралельно або в якості частини інших систем управління, як наприклад, система управління якістю, захисту навколишнього середовища та інформаційною безпеки (у такому випадку організація може звернутися до Стандартів ISO 9001, ISO 14001 та ISO/IEC 27001), а також Стандартів ISO 26000 і ISO 31000.

А.2.2. Сприяння та відступні

А.2.2.1. «Платежі з метою сприяння» – це термін, який подекуди використовується для визначення незаконних чи неофіційних платежів для отримання послуг, які платник має право законно отримати і без таких виплат. Зазвичай це порівняно незначна сума, яка сплачується державному службовцю або особі, що займається сертифікацією, для забезпечення або прискорення виконання рутинних або необхідних дій, як наприклад, видача візи, дозволу на роботу, розмитнення чи встановлення телефону. Хоча платежі з метою сприяння часто відрізняються за своєю природу від, наприклад, хабара, який сплачується для отримання ділової вигоди, у більшості країн вони вважаються незаконними і в рамках даного документу розглядаються в якості хабарів. Такі платежі також слід забороняти в рамках системи управління протидією хабарництву організації.

А.2.2.2. «Відступні платежі» – це той випадок, коли гроші силою вимагаються в персоналу шляхом реальних або потенційних загроз здоров'ю, безпеці чи свободі особи, і вони виходять за рамки даного документу. Безпека й свобода особи вважаються вищою цінністю, і в багатьох країнах законодавство не криміналізує випадки сплати таких платежів особами, які обґрунтовано бояться за власне здоров'я, безпеку чи свободу або ж здоров'я, безпеку й свободу іншої особи. Організація має можливість розробити політику, яка б дозволяла персоналу сплачувати такі виплати за умови існування обставин, коли працівники реально

бояться неминучою небезпеки власному здоров'ю, безпеці чи свободі або ж здоров'ю, безпеці чи

свободі іншої особи.

A.2.2.3. Організації слід надати конкретні настанови для будь-якого персоналу, який може стикатися із запитами або вимогами таких платежів, щодо способів їх уникнення або вирішення подальших проблемних питань. Такі настанови можуть включати в себе, наприклад, наступне:

а. конкретні заходи, яких рекомендується вжити будь-якому персоналу, що стикається з вимогами здійснити платіж:

1) у випадку з платежами з метою сприяння: запитати про докази законності платежу, офіційну квитанцію про оплату, а у випадку відсутності належних доказів – відмовитися від здійснення такого платежу;

2) у випадку з відступними платежами: здійснити оплату в тому випадку, коли існує загроза їх здоров'ю, безпеці або свободі або ж загроза здоров'ю, безпеці або свободі іншої особи;

б. конкретні заходи, яких рекомендується вжити будь-якому персоналу, який здійснив платіж з метою сприяння або відступний платіж:

1) зафіксувати подію;

2) повідомити про подію відповідному керівникові або Підрозділу забезпечення нормативно-правової відповідності;

в. конкретні заходи, яких рекомендується вжити організації, коли її персонал здійснив платіж з метою сприяння або відступний платіж:

1) призначити відповідного керівника для проведення розслідування даного випадку (бажано з Підрозділу забезпечення нормативно-правової відповідності або керівника, який вважається незалежним від департаменту або підрозділу причетного персоналу);

2) належним чином зафіксувати платіж у бухгалтерській звітності організації;

3) якщо вважається за потрібне, або якщо це вимагається чинним законодавством – повідомити про такий платіж відповідні органи влади.

A.3. Обґрунтованість і пропорційність

A.3.1. Хабар зазвичай вважається прихованим платежем. Його може бути складно попередити, зафіксувати чи відреагувати на нього. Зважаючи на такі ускладнення, загальним наміром даного документу вважається те, що керівному органу (якщо такий є) і вищому керівництву організації потрібно:

— мати реальне бажання попередити, зафіксувати та відреагувати на факти хабарництва, що стосуються справ або діяльності організації;

— мати реальні наміри з реалізації в рамках організації заходів, які було розроблено для попередження, фіксування й реагування на факти хабарництва.

Такі заходи не можуть бути надто дорогими, обтяжливими й бюрократичними, щоб їх не можна було б собі дозволити, або які б могли призупинити ділову діяльність організації. Вони також не можуть бути надто простими чи неефективними, що дозволяло б легко практикувати хабарництво. Потрібно, щоб заходи відповідали ризикам хабарництва, і слід, щоб вони мали обґрунтований шанс на успіх стосовно упередження, фіксування й реагування на факти хабарництва.

A.3.2. У той час, як типи заходів на протидію хабарництву, які планується реалізовувати, достатньо добре визнаються належною міжнародною практикою, а деякі з них відображені в

якості вимог даного документу, детальна інформація про такі заходи значним чином відрізняється для різних обставин. Неможливо вказати детальну процедуру, яку слід реалізувати організації у кожній окремій ситуації. Поняття «обґрунтованості й пропорційність» було введено в даний документ для того, щоб на їх основі оцінювались конкретні обставини справи.

A.3.3. Нижче приведено кілька прикладів застосування понять «обґрунтованості й пропорційності» в різних обставинах.

а. Дуже велика міжнаціональна організація може часто мати справу з кількома рівнями керівництва й тисячами найманих працівників. Зазвичай система управління протидією хабарництву такої організації потребуватиме значно глибшої деталізації ніж невеличке підприємство з кількома працівниками.

б. Організація, діяльність якої стикається зі значно вищими ризиками хабарництва (зважаючи на розташування), потребуватиме значно більш комплексної оцінки ризиків хабарництва та процедур комплексної перевірки «due diligence» й вищого рівня контролю протидією хабарництву за своїми правочинами на відміну від організації, яка провадить свою діяльність виключно в місцях, де ризик хабарництва порівняно низький.

в. Хоча ризик хабарництва існує стосовно багатьох правочинів або видів діяльності, процедури комплексної перевірки «due diligence» та контролю за протидією хабарництву, які реалізуються організацією, що займається масштабними правочинами чи діяльністю високої вартості за участі великої кількості ділових партнерів, швидше за все, будуть більш комплексними ніж ті, які реалізуються організацією, що займається продажем товарів низької вартості численним замовникам або провадить значну кількість незначних правочинів з одною стороною-учасником.

г. Організація зі значною кількістю ділових партнерів у рамках своєї оцінки ризиків хабарництва може прийти до висновку, що певні категорії ділових партнерів, наприклад, роздрібні покупці, менш вірогідно становитимуть ризик хабарництва зі ступенем вище «низького», і вона зважатиме на це протягом розробки й реалізації своєї системи управління протидією хабарництву. Наприклад, у такому випадку може не знадобитися комплексна перевірка «due diligence» або ж пропорційний чи обґрунтований контроль стосовно роздрібних клієнтів, які купують споживчі товари в організації.

A.3.4. Хоча ризик хабарництва стосується багатьох правочинів, організації радше слід реалізувати більш комплексний рівень контролю за протидією хабарництву для правочинів із високим рівнем хабарництва ніж низьким. У даному контексті важливо зрозуміти, що визначення й прийняття низького ризику хабарництва необов'язково означає, що організація приймає сам факт хабарництва, тобто ризик хабарництва (коли хабар МОЖУТЬ давати) – це не одне й те саме, що й безпосередній факт хабара. Організація спроможна мати «нульову терпимість» до хабарництва, але все одно вести справи в ситуаціях з низьким або вищим за низький ступінь хабарництва (допоки застосовуються належні заходи з мінімізації ризиків). Подальші настанови щодо конкретних засобів контролю приведено нижче.

A.4. Оцінка ризику хабарництва

A.4.1. Метою оцінки ризиків хабарництва, яка вимагається Пунктом 4.5, вважається надання організації можливості сформувати серйозну основу для власної системи управління протидією хабарництву. Така оцінка виявляє ризики хабарництва, на яких буде зосереджено систему управління, тобто ризики хабарництва, які вважаються пріоритетними для організації, з метою мінімізації таких ризиків, реалізації контролю й розподілу персоналу з підрозділів, які займаються боротьбою з хабарництвом, ресурсів і заходів. Те, яким чином проводиться оцінка ризиків хабарництва, яка методологія застосовується, яким чином зважуються й отримуються пріоритети ризиків, а також рівень прийнятності (тобто «схильність до ризику») або сприйняття ризиків – усе це лишається на розсуд організації. Зокрема саме організація створює власні критерії оцінки ризику хабарництва (наприклад, «низького», «середнього» або «високого» ризику); проте при цьому організація також повинна

 зважати на свою політику й цілі протидії хабарництву.

Нижче приведено приклади того, яким чином організація може проводити таку оцінку.

а. Вибір критеріїв оцінки ризиків хабарництва. Наприклад, організація може обрати «трьохступеневі» критерії (тобто «низького», «середнього» або «високого» ризику), детальніші п'ятиступеневі або семиступеневі критерії, або ж навіть ще детальніший підхід. Такі критерії часто зважатимуть на кілька факторів, включаючи природу ризику хабарництва, вірогідність випадку хабарництва та вагомість наслідків, якщо факт хабара матиме місце.

б. Оцінка ризиків хабарництва, які залежать від розміру й структури організації. Невелика

організація, розташована в одному місці з централізованими засобами контролю в руках кількох осіб, може спромогтися контролювати ризики хабарництва значно простіше аніж дуже велика організація з децентралізованою структурою, яка працює в численних місцях.

в. Перевірка місць розташування й секторів, у яких працює або ж планує працювати організація, а також оцінка ступеня ризику хабарництва, який можуть становити такі місця розташування або сектори. Місця або сектори з високим ризиком хабарництва можуть вважатися організацією «низьким», «середнім» або «високим» ризиком. Це може призвести до того, що організація, наприклад, застосовує вищий рівень контролю до своєї діяльності в таких місцях розташування або секторах.

г. Перевірка природи, масштабів та складності типів діяльності й операцій організації.

1) Наприклад, може виявитися простішим контролювати ризик хабарництва, коли організація займається незначним виробництвом в одному місці, ніж коли вона має справу з кількома будівельними проектами в кількох місцях.

2) Деякі типи діяльності можуть мати конкретні ризики хабарництва, наприклад, компенсаційні домовленості, у рамках яких урядом закуповуються товари або послуги, які вимагають від постачальника реінвестицій певної частини вартості контракту в країні, що закуповує. Організації слід вжити відповідних заходів для упередження випадків хабарництва в рамках таких компенсаційних домовленостей.

д. Перевірка чинних і потенційних типів ділових партнерів організації за категоріями, а також оцінка принципових ризиків хабарництва, які вони можуть становити. Наприклад:

1) Організація може мати значну кількість клієнтів, які купують продукти наднизької вартості в організації, що на практиці становить для організації мінімальний ризик хабарництва. У даному випадку організація може вважати ризик таких клієнтів «низьким» і може постановити, що стосовно таких клієнтів непотрібно застосовувати конкретних засобів контролю запобігання хабарництву. І навпаки – організація може мати справу з замовниками, які купують високовартісні товари в організації, що може становити значний ризик хабарництва (тобто ризик вимагання хабарів від організації в обмін на оплату і її затвердження). Такі типи клієнтів можуть становити «середній» або «високий» ступінь ризику, і вони можуть потребувати вищого рівня контролю протидії хабарництва збоку організації.

2) Різні типи постачальників можуть становити різні ступені ризику хабарництва. Наприклад, постачальники зі значним об'ємом робіт або ж ті, що контактують із клієнтами й замовниками організації та відповідними державними службовцями, можуть становити «середній» або «високий» рівень хабарництва. Деякі категорії постачальників можуть становити «низький» ризик, тобто розташовуватися в місцях із низьким рівнем ризику хабарництва і не мати зв'язків із відповідними державними службовцями, клієнтами або замовниками організації. Інші категорії постачальників можуть становити «дуже низький» ступінь ризику хабарництва, наприклад, коли вони постачають незначні кількості товарів або товари низької вартості, онлайн-послуги із придбання авіа квитків чи бронювання готелів. Організація може прийти до висновку, що стосовно таких постачальників із

«низьким» або «дуже низьким» ступенем ризику хабарництва можна не застосовувати певні засоби контролю протидії хабарництву.

3) Агенти й посередники, які взаємодіють із клієнтами організації чи державними службовцями від імені організації, швидше за все, становитимуть «середній» або «високий» ступінь ризику хабарництва, зокрема якщо їм сплачуються комісійні чи гонорари у випадку успішності їх діяльності.

е. Перевірка природи й частоти взаємодії з національними й закордонними державними службовцями, які можуть становити ризик хабарництва, наприклад, взаємодія з державними службовцями, відповідальними за видачу дозволів і затверджень, може становити саме такий ризик.

ж. Перевірка застосовних статутних, нормативних, контрактних і професійних зобов'язань та обов'язків, наприклад, заборона або обмеження залучення державних службовців або використання послуг агентів.

з. Перевірка межі, до якої організація спроможна впливати або контролювати оцінені ризики.

Вказані вище фактори ризику хабарництва взаємопов'язані. Наприклад, постачальники з одної категорії можуть становити різні ступені ризику залежно від місця свого розташування.

A.4.2. Оцінивши відповідні ризики хабарництва, організація може визначати тип і рівень засобів контролю протидії хабарництву, які застосовуються до кожної категорії ризиків, а також спроможна оцінити адекватність чинних засобів контролю. Якщо ж ні, вона спроможна відповідним чином удосконалити засоби контролю. Наприклад, вищий рівень контролю, швидше за все, буде реалізовуватися стосовно місць розташування із вищим ступенем ризику хабарництва та вищими категоріями ризику хабарництва серед ділових партнерів. Організація може ухвалити рішення стосовно застосування нижчого рівня контролю за діяльністю або діловими партнерами із «низьким» ступенем ризику. Деякі вимоги даного документу чітко виключають потребу в застосуванні таких вимог до видів діяльності або ділових партнерів із «низьким» ступенем ризику (хоча організація може обрати варіант із їх застосуванням, якщо вона того забажає).

A.4.3. Організація спроможна змінити природу правочину, проекту, діяльності або відносин задля мінімізації природи й масштабів ризику хабарництва таким чином, щоб ним можна було належним чином керувати за допомогою існуючих, удосконалених або додаткових засобів контролю за протидією хабарництву.

A.4.4. Ця практична вправа з оцінки ризику хабарництва не ставить собі за мету бути вичерпною або надто комплексною, а результати оцінки необов'язково мають виявитись коректними (наприклад, правочин, оцінений «низьким» ступенем ризику хабарництва, може виявитися таким, що має під собою факт хабара). Наскільки це реально можливо, результати оцінки ризиків хабарництва мають відображати реальні ризики хабарництва, з якими має справу організація. Цю вправу слід спроектувати таким чином, щоб її можна було використати в якості інструменту на підтримку оцінки та встановлення пріоритетів щодо ризиків хабарництва, і її слід регулярно переглядати й поновлювати на базі змін в організації чи обставинах (наприклад, нові ринки або товари, законні вимоги та отриманий досвід).

ПРИМІТКА: Подальші настанови можна знайти в Стандарті ISO 31000.

A.5. Функції та відповідальність керівного органу й вищого керівництва

A.5.1. Численні організації мають певну форму керівного органу (наприклад, рада директорів або наглядова рада), що мають певні обов'язки з нагляду за діяльністю організації. Такі обов'язки включають у себе нагляд за системою управління протидією хабарництву організації. Проте керівні органи зазвичай не займаються повсякденним контролем за діяльністю організації. Це функція виконавчого керівництва (наприклад, головного виконавчого директора чи головного операційного директора), яке в рамках даного

документу визначається, як «вище керівництво». Що стосується системи управління протидією хабарництву, керівному органу слід бути обізнаному про склад і роботу системи управління, а також слід здійснювати обґрунтований нагляд за адекватністю, ефективністю й реалізацією системи управління. Слід регулярно отримувати інформацію про виконання системи управління через процес огляду системи управління (що може стосуватися всього керівного органу або його комітету, як наприклад, аудиторського комітету). У даному питанні Підрозділу забезпечення нормативно-правової відповідності слід мати потенціал
повідомляти інформацію про систему управління безпосередньому керівному органу (або його відповідному комітету).

A.5.2. Деякі організації, зокрема невеликі, можуть не мати окремого керівного органу або підрозділів керівного органу, а виконавче керівництво може бути представленим одною групою осіб або навіть одною особою. У таких випадках група осіб або особа виконуватиме обов'язки, окреслені даним документом для вищого керівництва й керівного органу.

ПРИМІТКА: Зобов'язання керівництва іноді називаються «особистим прикладом керівництва» або «тоном, що задається нагорі».

A.6. Підрозділ забезпечення нормативно-правової відповідності

A.6.1. Кількість людей, які працюють у Підрозділі забезпечення нормативно-правової відповідності, залежить від таких факторів, як розмір організації, масштаби ризику хабарництва, з якими стикається організація, а також відповідного робочого навантаження на підрозділ. У невеличких організаціях Підрозділ забезпечення нормативно-правової відповідності може бути представленим одною особою, уповноваженою виконувати свої функції на тимчасовій основі, суміщаючи такі функції з іншими обов'язками. У випадку обґрунтування цього ризиком хабарництва та відповідним робочим навантаженням, Підрозділ забезпечення нормативно-правової відповідності має можливість бути представленим одною особою, уповноваженою на роботу на повній ставці. У великих організаціях у такому підрозділі зазвичай працює кілька людей. Деякі організації можуть доручати таку функцію комітету з широким і відповідним робочим досвідом. Деякі організації мають можливість скористатися послугами третьої сторони для виконання деяких або всіх функцій Підрозділу забезпечення нормативно-правової відповідності, і це вважається прийнятним за умови, що відповідний керівник у самій організації лишає за собою загальну відповідальність та повноваження Підрозділу забезпечення нормативно-правової відповідності, а також здійснює нагляд за послугами, які надаються третьою стороною.

A.6.2. Даний документ вимагає, щоб у Підрозділі забезпечення нормативно-правової відповідності працювала(и) особа(и) належної компетентності, статусу, повноважень і незалежності. У даному випадку:

а. «компетентність» означає, що певна особа(и) має належну освіту, підготовку й досвід, а також особисту здатність виконувати вимоги до своїх функцій, а також потенціал навчатися виконувати певну функцію та належне її виконання;

б. «статус» означає, що інший персонал, швидше за все, дослухатиметься й поважатиме думки особи, яка виконує функції Підрозділу забезпечення нормативно-правової відповідності;

в. «повноваження» означає, що відповідна(і) особа(а) наділена повноваженнями керівним органом (якщо такий є) і вищим керівництвом, які можна вважати достатніми для ефективного виконання функцій такого підрозділу;

г. «незалежність» означає, що певна(і) особа(и), яка уповноважена на виконання функцій Підрозділу забезпечення нормативно-правової відповідності, наскільки це можливо, не бере особистої участі в діяльності організації, що стикається з ризиком хабарництва. Цього простіше досягти, коли організація призначає особу на виконання функцій на постійній і повноцінній основі, але такі можливості можуть бути недоступними для маленької організації, у якій така особа суміщає функцію Підрозділу забезпечення

нормативно-правової відповідності з іншими обов'язками. В останньому випадку функцію Підрозділу забезпечення нормативно-правової відповідності не слід доручати особі, яка підпадає під ризик хабарництва протягом виконання своїх основних обов'язків. У випадку з дуже великими організаціями, коли незалежності досягти складніше, відповідній(им) особі(ам) слід, наскільки це можливо, відділити всі свої інші обов'язки від функцій Підрозділу забезпечення нормативно-правової відповідності задля забезпечення власної неупередженості.

A.6.3. Важливо, щоб Підрозділ забезпечення нормативно-правової відповідності мав прямий доступ до вищого керівництва й керівного органу (якщо такий є) для комунікації відповідної інформації. Підрозділу не слід звітувати виключно перед іншим керівником у ланцюгу підпорядкування, учасники якого потім звітують перед вищим керівництвом, адже це підвищує ризик неповної або неточної передачі повідомлення Підрозділу забезпечення нормативно-правової відповідності для вищого керівництва. Підрозділу забезпечення нормативно-правової відповідності також слід мати прямий зв'язок із керівним органом (якщо такий є) без необхідності проходити через усе вище керівництво. Це може бути або повністю сформований керівний орган (наприклад, рада директорів або наглядова рада), або ж спеціально делегований комітет керівного органу або вищого керівництва (наприклад, комітет із питань аудиту або етики).

A.6.4. Основним обов'язком Підрозділу забезпечення нормативно-правової відповідності вважається нагляд за формуванням та реалізацією системи управління протидією хабарництву. Його не слід плутати з безпосередніми обов'язками щодо боротьби з хабарництвом в організації а також

відповідності застосовному законодавству з питань протидії хабарництву. Усі працівники відповідальні за власну етичну й відповідну поведінку, що включає в себе відповідність вимогам системи управління протидією хабарництву організації та законам із питань протидії хабарництву. Зокрема важливо, щоб керівництво взяло на себе провідну роль у досягненні нормативно-правової відповідності в тих частинах організації, за які вони несуть відповідальність.

ПРИМІТКА: Подальші настанови можна знайти в Стандарті ISO 19600.

A.7. Ресурси

Потрібні ресурси залежать від таких факторів, як розмір організації, природа її діяльності та ризики хабарництва, з якими вона стикається. Такі ресурси включають у себе наступне.

а. **Кадрові ресурси:** Слід забезпечити належну кількість персоналу, спроможного присвятити достатньо часу відповідним функціям із протидії хабарництву для ефективного функціонування системи управління протидією хабарництву. Це включає в себе призначення достатньої кількості осіб (зовнішніх або внутрішніх) до Підрозділу забезпечення нормативно-правової відповідності.

б. **Матеріальні ресурси:** В організації слід забезпечити достатню кількість матеріальних ресурсів, які включають ресурси для забезпечення ефективної роботи Підрозділу забезпечення нормативно-правової відповідності й системи управління протидією хабарництву, наприклад, офісні приміщення, меблі, комп'ютерне апаратне й програмне забезпечення, матеріали для тренінгів, телефонія та канцелярське приладдя.

в. **Фінансові ресурси:** Слід забезпечити достатній бюджет для ефективного функціонування Підрозділу забезпечення нормативно-правової відповідності й системи управління протидією хабарництву.

A.8. Процес найму

A.8.1. Комплексна перевірка «due diligence» персоналу

Протягом комплексної перевірки («due diligence») осіб перед їх призначенням на кадрові посади організація має можливість вжити наступних заходів залежно від посад, які

 пропонуються, і відповідних ризиків

хабарництва:

а. обговорення політики протидії хабарництву організації із потенційним персоналом протягом співбесід, а також формування бачення того, чи вони можуть зрозуміти й сприйняти важливість питання відповідності;

б. реалізація обґрунтованих кроків для перевірки точності вказаної кваліфікації потенційного персоналу;

в. реалізація обґрунтованих кроків для отримання задовільних рекомендацій від попередніх роботодавців потенційного персоналу;

г. реалізація обґрунтованих кроків для визначення можливої причетності потенційного персоналу до випадків хабарництва;

д. реалізація обґрунтованих кроків для перевірки того, чи не пропонує організація роботу потенційному персоналу в обмін на послуги, які такі працівники могли надавати протягом своєї роботи на попередньому місці, що можна вважати незаслуженою перевагою;

е. перевірки можливості того, що пропозицію роботи потенційному персоналу не можна вважати демонстрацією необґрунтованої прихильності організації до певних кандидатів;

ж. реалізація обґрунтованих кроків для виявлення зв'язків потенційного персоналу з державними службовцями.

A.8.2. Показники ефективності (виконання)

Механізми компенсації, які включають у себе преміальні й заохочення, можуть спровокувати персонал, навіть ненавмисно, до участі в хабарництві. Наприклад, якщо керівник отримає премію за передачу контракту організації, такий керівник може постати перед спокусою заплатити хабара або ж

навмисно не звернути уваги на сплату хабара агентом чи діловим партнером для гарантованого отримання контракту. Аналогічний випадок може трапитися, якщо на керівника занадто тиснуть через ефективність його/її роботи (наприклад, якщо керівника можуть звільнити через невдачу із досягненням надто амбіційних цілей із продажу). Організації потрібно бути дуже уважною з такими аспектами компенсації задля забезпечення того, щоб вони не стали мотивацією для отримання чи сплати хабара.

Оцінка персоналу, підвищення, премії та інші типи винагороди можна використати в якості мотивації персоналу до належного виконання ними своїх обов'язків відповідно до політики протидії хабарництву й системи управління протидією хабарництву організації. Проте в даному випадку організації потрібно бути обережною, адже загроза втратити премію, тощо, може стати причиною приховування невдач системи управління протидією хабарництву персоналом.

Персонал слід повідомити про те, що порушення вимог системи управління протидією хабарництву для покращення виконання робіт в інших сферах (наприклад, для досягнення цілей із продажів) вважається неприйнятним, і їх слід виправляти і/або вживати відповідних дисциплінарних заходів.

A.8.3. Конфлікти інтересів

Організації слід визначити й оцінити ризик внутрішнього й зовнішнього конфлікту інтересів. Організації слід чітко проінформувати весь персонал про їх обов'язок повідомляти про будь який реальний або потенційний конфлікт інтересів, як наприклад, сімейні, фінансові або інші зв'язки, що можуть безпосередньо або опосередковано впливати на їх сферу зайнятості. Це допомагає організації виявити ситуації, коли персонал може сприяти або відмовлятися повідомляти про факти хабарництва, як наприклад:

а. коли менеджер із продажів організації має зв'язки з менеджером із питань закупівель клієнта; або

б. коли лінійний керівник організації має особисту фінансову зацікавленість у бізнесі конкурента.

Організації слід вести записи щодо всіх обставин реального чи потенційного конфлікту інтересів, а також заходів щодо мінімізації таких конфліктів (якщо такі були).

A.8.4. Хабарництво збоку персоналу організації

A.8.4.1. Заходи, необхідні для упередження, виявлення й усунення ризиків хабарництва щодо інших осіб від імені організації збоку персоналу організації («вихідне хабарництво»). Можуть відрізнятися від заходів, що вони вживаються для упередження, виявлення й усунення ризиків хабарництва щодо персоналу організації («вхідне хабарництво»). Наприклад, здатність виявляти та мінімізувати ризик вхідного хабарництва можна значним чином обмежити наявністю інформації, що виходить за межі контролю організації (наприклад, особистий банківський рахунок найманого працівника або виписка по його/її кредитній картці), застосовним правом (наприклад, закон про приватну інформацію) або іншими факторами. У результаті кількість і типи засобів контролю, якими організація оперує для мінімізації ризику вихідного хабарництва, можуть бути більшими за кількість засобів контролю, якими оперує така організація для мінімізації вхідного хабарництва.

A.8.4.2. Частіше за все хабарництво стосовно персоналу організації може відбуватися щодо працівників, які мають можливість ухвалювати рішення або впливати на процес їх ухвалення від імені організації (наприклад, менеджер із питань закупівель, уповноважений підписувати контракти; начальник, який затверджує пророблену роботу; менеджер, уповноважений призначати персонал або затверджувати зарплатню чи премії; клерк, який готує документацію для видачі ліцензій і дозволів). У випадках, коли хабар приймається персоналом поза сферою впливу систем і засобів контролю організації, здатність організації упереджувати чи фіксувати такі хабарі може бути обмеженою.

A.8.4.3. На додачу до кроків, описаних у A.8.1 і A.8.3, ризик вхідного хабарництва можливо мінімізувати наступними вимогами даного документу, що стосуються даного ризику:

а. у політиці протидії хабарництву організації (див. 5.2) слід чітко визначати заборону сприяння або приймання хабарів персоналом організації та будь-ким, хто працює від її імені;

б. через настанови й матеріали для тренінгів (див. 7.3) слід посилювати заборону сприяння або приймання хабарів, і вони повинні містити наступне:

1) настанови щодо повідомлення про можливі випадки хабарництва (див. 8.9); 2) акцент на політиці захисту співробітників організації від переслідування (див. 8.9);

в. у політику організації щодо подарунків і проявів гостинності (див. 8.7) слід внести обмеження для персоналу щодо приймання подарунків і проявів гостинності;

г. через публікацію на офіційному вебсайті організації політики протидії хабарництву та детальної інформації про те, як повідомлення про хабарництво допомагають встановити очікування від ділових партнерів щодо мінімізації вірогідності пропонування хабарів такими діловими партнерами або ж приймання таких хабарів чи сприяння й їх прийманні персоналом організації;

д. засоби контролю (див. 8.3 і 8.4), що вимагають, наприклад, користуватися послугами затверджених постачальників, конкурентними ціновими пропозиціями, принаймні двома підписами на документах про присудження контрактів, затвердження робіт, тощо, для мінімізації ризиків корумпованих передач контрактів, затверджень, виплат чи переваг.

A.8.4.4. Організація також може займатися реалізацією процедур аудиту для виявлення шляхів використання персоналом існуючих недоліків контролю для отримання особистої вигоди. Прикладом таких процедур можуть бути:

 а. аналіз платіжних відомостей на предмет «мертвих душ» або дублікатів; б. аналіз записів про витрати персоналу для виявлення незвичайних видатків;

в. порівняння інформації у платіжних відомостях персоналу (наприклад, номерів особистих банківських рахунків і адрес) з інформацією про банківські рахунки й адреси в головному файлі постачальників організації для виявлення сценаріїв потенційних конфліктів інтересів.

A.8.5. Тимчасовий персонал або робітники

У деяких випадках тимчасовий персонал або працівники можуть підшукуватися організації кадровим агентством або іншим діловим партнером. У такому випадку організації слід визначити, чи належним чином ставляться до ризику хабарництва, який можуть становити такий тимчасовий персонал або робітники (якщо такий ризик існує) шляхом відношення до тимчасового персоналу й робітників, як до постійного штату, з огляду на підготовку й контроль, або ж є необхідність у застосуванні відповідних засобів контролю через ділового партнера, який надає такий тимчасовий персонал або робітників.

A.9. Інформування та навчання

A.9.1. За мету навчання вважається допомога в забезпеченні розуміння персоналом наступних факторів відповідно до їх функцій в організації:

а. ризики хабарництва, з якими стикаються вони особисто або їх організація; б. політика протидії хабарництву;

в. аспекти системи управління протидією хабарництву, що стосуються їх функцій;

г. будь-які необхідні заходи для упередження й звітування, яких слід вжити щодо будь якого ризику хабарництва або підозри щодо хабарництва.

A.9.2. Формальність та масштаби навчання залежать від розміру організації й ризиків хабарництва, з якими вона стикається. Навчання можна проводити в рамках онлайн модуля або ж очно (наприклад, класні заняття, практикуми, круглі столи, дискусії відповідного персоналу та персональні заняття). Метод навчання менш важливий за його результати, за якими всьому відповідному персоналу слід зрозуміти питання, на які посилаються в A.9.1.

A.9.3. Очне навчання рекомендується для керівного органу (якщо такий є) та будь-якого персоналу (незалежно від їх посад або внутрішньої ієрархії організації) та ділових партнерів, яких залучено до операцій і процесів зі ступенем ризику вище «низького».

A.9.4. Якщо відповідний персонал, уповноважений на виконання функцій Підрозділу забезпечення нормативно-правової відповідності, не має відповідного робочого досвіду, організації слід

забезпечити його/її відповідне навчання для належного виконання нею/ним функцій Підрозділу забезпечення нормативно-правової відповідності.

A.9.5. Навчання може проводитися у вигляді автономного тренінгу з протидії хабарництву або бути частиною загального навчання організації з питань забезпечення відповідності й етики чи вступного курсу.

A.9.6. Склад (контент) курсу можна адаптувати під функції персоналу. Персонал, що не стикається зі значним ризиком хабарництва протягом виконання своїх функцій, може пройти найпростіший тренінг з політики організації для розуміння останньої, а також щоб знати, що робити у випадку потенційного порушення. Персоналу, функції якого підпадають під високий ризик, слід пройти детальнішу підготовку.

A.9.7. Підготовку слід проводити регулярно для того, щоб персонал був у курсі чинної

політики й процедур організації, а також будь-яких питань розвитку своїх функцій чи будь яких нормативних змін.

A.9.8. Застосування вимог до навчання та інформування стосовно ділових партнерів, визначених 7.3, становить окремий виклик, адже наймані працівники таких ділових партнерів зазвичай не працюють на організацію напряму, і організація зазвичай не має безпосереднього впливу на таких працівників з метою проведення навчання. Реальне навчання найманих працівників, що працюють на ділових партнерів, зазвичай проводиться самими діловими партнерами або іншими сторонами, послуги яких залучаються саме з цією метою. Важливо, щоб робітники, які працюють на ділових партнерів і можуть стикатися з ризиком хабарництва для організації зі ступенем вище «низького», були проінформовані про це питання й пройшли належне навчання для мінімізації ризику. Зміст 7.3 вимагає від організації, як мінімум, виявити ділових партнерів, чиї наймані працівники повинні пройти підготовку з протидії хабарництву, інформування про мінімальний зміст такої підготовки й необхідність її проведення. Сама підготовка може надаватися діловим партнером, визначеною третьою стороною або, якщо того бажає організація, самою організацією.

Організація має можливість комунікувати про такі зобов'язання з діловими партнерами за допомогою різних засобів, включаючи й ті, що вважаються складовими відповідних контрактних домовленостей.

A.10. Комплексна перевірка «due diligence»

A.10.1. Метою проведення комплексної перевірки «due diligence» щодо певних правочинів, проектів, діяльності, ділових партнерів або персоналу організації вважається подальша оцінка сфери застосування, масштабів і природи ризиків хабарництва зі ступенем вище «низького», що їх було виявлено протягом оцінки ризиків організації (див. 4.5). Вона також грає роль додаткового цільового контролю в процесі упередження й виявлення ризику хабарництва, а також для інформування про рішення організації стосовно відкладення, припинення чи перегляду таких правочинів, проектів або відносин із діловими партнерами чи персоналом.

Що стосується проектів, правочинів та діяльності, для організації може бути корисним включити до оцінки:

а. структуру, природу й складність (наприклад, прямі чи опосередковані продажі, рівень знижки, передача контракту й процедури проведення тендеру);

б. фінансові й платіжні домовленості;

в. об'єм робіт організації та доступні ресурси;

г. рівень контролю й візуалізації;

д. ділових партнерів та їх залучених третіх сторін (включаючи державних службовців); е.

зв'язки між сторонами пункту д) вище й державними службовцями;

ж. компетенцію й кваліфікацію залучених сторін;

з. репутацію клієнта;

и. місце розташування;

к. повідомлення на ринку або в пресі.

Що стосується можливості проведення комплексної перевірки «due diligence» ділових партнерів:

а. для організації може бути корисним включити до оцінки ділових партнерів наступні фактори:

1) чи діловий партнер вважається законно зареєстрованою юридичною особою, на що вказують такі індикатори, як установчі документи, щорічна фінансова звітність,

ідентифікаційний номер платника податків, допуск його цінних паперів до торгів на біржі, тощо;

2) чи має діловий партнер достатню кваліфікацію, досвід та ресурси, потрібні для ведення справ, для яких із таким партнером було підписано контракт;

3) чи має діловий партнер систему управління протидією хабарництву та її масштаби;

4) чи має діловий партнер репутації щодо випадків хабарництва, шахрайства, недобросовісної поведінки або аналогічних порушень; чи знаходився діловий партнер під слідством, був засуджений, обкладений санкціями або відсторонений через випадки хабарництва або аналогічні кримінальні порушення;

5) особистість акціонерів (включаючи реальних бенефіціарних власників та вищого керівництва ділового партнера, а також чи вони:

і) мають репутацію щодо випадків хабарництва, шахрайства, недобросовісної поведінки або аналогічних порушень;

іі) знаходилися під слідством, були засуджені, обкладені санкціями або відсторонені через випадки хабарництва або аналогічні кримінальні порушення;

ііі) мають прями чи опосередковані зв'язки з клієнтами або замовниками організації чи відповідними державними службовцями, що може призвести до хабарництва (така категорія включає в себе осіб, які самі можуть не бути державними службовцями але можуть бути прямо чи опосередковано пов'язаними з державними службовцями, кандидатами на державну посаду, тощо);

6) структура правочину та платіжних домовленостей;

б. природа, тип і масштаби запланованої комплексної перевірки «due diligence» залежатимуть від таких факторів, як здатність організації отримувати достатню кількість інформації, вартість отримання інформації та ступінь можливого ризику хабарництва, яке становлять чинні відносини з діловими партнерами;

в. процедури комплексної перевірки «due diligence», які виконуються організацією щодо ділових партнерів, мають бути послідовними для всіх аналогічних ступенів ризику хабарництва (ділові партнери з високим ступенем ризику хабарництва, які працюють в місцях або на ринках з високим ступенем хабарництва, швидше за все, потребуватимуть значного рівня комплексної перевірки «due diligence» у порівнянні з діловими партнерами нижчого ступеня ризику, які працюють в місцях або на ринках із низьким ступенем ризику);

г. різні типи ділових партнерів, швидше за все, потребуватимуть різних рівнів комплексної перевірки «due diligence», наприклад:

1) з точки зору потенційної правової й фінансової відповідальності організації, ділові партнери становлять вищий ризик хабарництва для організації в тому випадку, коли вони виступають від імені організації або в її інтересах у порівнянні з тими випадками, коли ділові партнери надають організації товари або послуги. Наприклад, агент, залучений до підтримки організації для отримання певного контракту, також може заплатити хабара менеджеру клієнта організації задля допомоги організації з отриманням контракту, і це може спричинити відповідальність організації за корупційну діяльність агента. У результаті комплексна перевірка «due diligence» організації щодо агента, вірогідно, буде надзвичайно комплексною. З іншого боку, постачальник, який продає обладнання або матеріали організації, і який не має жодних стосунків із клієнтами організації або державними службовцями, менш вірогідно потребуватиме сплати хабара від імені організації або в її інтересах, а отже рівень перевірки «due diligence» такого постачальника може бути нижчим;

2) рівень впливу, що його має організація на своїх ділових партнерів, також впливає на здатність такої організації отримувати інформацію безпосередньо від ділових партнерів у рамках комплексної перевірки «due diligence». Це може бути відносно просто для організації вимагати від своїх агентів та партнерів за спільним

підприємством інформацію про них в рамках процедури «due diligence» до того, як брати на себе зобов'язання щодо роботи з ними, адже в такій ситуації сама організація може вирішувати з ким і коли підписувати контракт. Проте для організації може бути складнішим вимагати надання інформації або заповнення анкет комплексної перевірки «due diligence» від своїх замовників або клієнтів. Причиною тому може бути те, що організація може не мати достатнього впливу на клієнта або замовника для того, щоб ставити такі вимоги (наприклад, коли організація бере участь у конкурентному тендері для надання послуг замовнику);

д. комплексна перевірка «due diligence», яка проводиться організацією стосовно її ділових партнерів, може включати в себе, наприклад:

1) анкету, яка надсилається діловому партнеру, у якій його просять відповісти на питання, приведені в A.10.3 a);

2) пошук інформації про ділового партнера та його акціонерів і вищого керівництва в мережі Інтернет для отримання даних стосовно випадків хабарництва;

3) пошук потрібної інформації за відповідними урядовими, судовими та міжнародними ресурсами;

4) перевірка публічних списків відсторонених організацій, на яких накладено обмеження, або яким заборонено укладати мати договірні відносини з державними або урядовими органами, що ведуться національними або місцевими органами влади або ж такими міжнародними інституціями, як наприклад, Світовий Банк;

5) наведення довідок в інших сторін про етичну репутацію ділового партнера організації;

6) призначення інших осіб або організації з відповідним робочим досвідом на підтримку в процесі проведення комплексної перевірки «due diligence»;

е. діловому партнеру можна задавати подальші питання на основі результатів початкової комплексної перевірки «due diligence» (наприклад, щоб пояснити негативну інформацію).

A.10.4. Комплексну перевірку «due diligence» не можна вважати бездоганним інструментом. Відсутність негативної інформації необов'язково має означати, що діловий партнер не становить жодного ризику хабарництва. Негативна інформація необов'язково означає, що діловий партнер становить ризик хабарництва. Проте результати потребують ретельної о

цінки та раціонального обґрунтування збоку організації, що базуються на доступних фактах. Загальне прагнення полягає в тому, щоб організація робила обґрунтовані й пропорційні запити про ділового партнера, зважаючи на діяльність останнього та ризик, характерний для такої діяльності, щоб сформувати обґрунтоване судження про ступінь ризику хабарництва, з яким стикається організація у випадку роботи з таким діловим партнером.

A.10.5. Комплексна перевірка **«**due diligence» стосовно персоналу описана в A.8.1.

A.11. Фінансовий контроль

Фінансовий контроль – це системи й процеси управління, які реалізуються організацією для належного управління фінансовими правочинами й точного, повного і вчасного фіксування таких правочинів. Залежно від розмірів організації й правочину, фінансовий контроль, який реалізується організацією для мінімізації ризику хабарництва, може включати в себе, наприклад:

а. реалізацію розподілу обов'язків, щоб одна і та ж особа не могла ініціювати й затверджувати

виплати;

б. реалізацію відповідних ступенів або рівнів повноважень для затвердження виплат (щоб масштабніші правочини потребували затвердження збоку вищого рівня керівництва);

в. перевірку того, щоб призначення, робота й послуги одержувача платежів

 затверджувалися відповідними механізмами організації;

г. вимоги щодо принаймні двох підписів для затвердження виплат;

д. вимоги щодо відповідної супровідної документації, яка повинна додаватися до затверджень платежів;

е. обмеження на використання готівки та ефективні методи контролю готівкового обігу; ж.

вимоги щодо точної й чіткої категоризації виплат та їх опису на рахунках; з. реалізацію

регулярного аналізу важливих фінансових правочинів збоку керівництва;

и. проведення регулярних і незалежних фінансових аудитів та регулярних змін організацій або осіб, які займаються проведенням аудиту.

A.12. Не-фінансовий контроль

Не-фінансовий контроль – це системи й процеси управління, які реалізуються організацією для забезпечення належного управління закупівлями, оперативними, комерційними й іншими не фінансовими аспектами діяльності організації. Залежно від розмірів організації й правочину, контроль над закупівлями, оперативними, комерційними й іншими не-фінансовими аспектами діяльності організації для мінімізації ризиків хабарництва може включати в себе, наприклад:

а. використання затверджених підрядників, субпідрядників, постачальників і консультантів, які пройшли процес попередньої кваліфікації, за яким проводиться вірогідність їх участі в процесі хабарництва; такий процес, швидше за все, включатиме в себе комплексну перевірку «due diligence» того типу, на який посилаються в Статті A.10;

б. оцінку:

1) необхідності й законності послуг, які планує надавати організації діловий партнер (за виключенням замовників і клієнтів організації);

2) належного чину надання таких послуг;

3) обґрунтованості й пропорційності виплат на користь ділового партнера стосовно наданих ним послуг. Це зокрема важливо для того, щоб уникнути ризику використання діловим партнером частини таких коштів організації для сплати хабара від її імені або в її інтересах. Наприклад, у випадку призначення організацією агента на підтримку операцій із продажів, якому потрібно сплачувати певну комісію або гонорар за отриманий для організації контракт, організації слід переконатися в тому, що комісійні виплати обґрунтовані й пропорційні законним послугам, які надаються агентом, зважаючи на ризик, на який пристає агент у випадку не-підписання контракту. У випадку сплати непропорційно великих комісій або гонорарів існує підвищений ризик використання певної частини таких платежів агентом не за призначенням – для спонукання державного службовця або найманого працівника клієнтської організації до передачі певного контракту на користь організації. Організація такою може надіслати запит до ділового партнера й отримати документацію, яка підтверджує надання певних послуг;

в. можливості й обґрунтування передачі контрактів лише після проведення (якщо це вимагається) справедливого й прозорого тендерного процесу серед принаймні трьох учасників;

г. вимоги щодо призначення принаймні двох осіб для оцінки й затвердження процесу присудження контракту;

д. реалізації розподілу обов'язків, щоб персонал, який затверджує підписання контрактів, відрізнявся від того, який надсилає запити щодо підписання контракту, а також належав до підрозділу чи департаменту, які не займаються управлінням контракту і не затверджують робіт, виконаних за контрактом;

е. вимоги щодо підписів принаймні двох осіб на контрактах, а також документах про

внесення змін до контрактів, або ж осіб, які затверджують виконані роботи або передані товари за контрактом;

ж. застосування вищого рівня управлінського нагляду за правочинами із потенційно вищим ступенем ризику;

з. захисту доброчесності тендерів та іншої інформації, чутливої до цінових питань шляхом обмеження доступу виключно для відповідного персоналу;

и. надання відповідного інструментарію й шаблонів для підтримки персоналу (наприклад, практичних настанов, «плюсів і мінусів», ієрархій процесу затвердження рішень, контрольних списків, форм, IT робочих потоків, тощо).

ПРИМІТКА: Із подальшими прикладами засобів контролю й настановами можна ознайомитися в Стандарті ISO 19600.

A.13. Реалізація системи управління протидією хабарництву підконтрольними організаціями й діловими партнерами

A.13.1. Загальна інформація

Причина вимоги Статті 8.5 полягає в тому, що підконтрольні організації й ділові партнери можуть становити ризик хабарництва для організації. Типи ризиків хабарництва, яких у даних випадках прагне уникнути організація, включають у себе, наприклад:

а. сплату хабара філіалом організації, у результаті чого відповідальність може понести сама організація;

б. сплату хабара спільним підприємством або партнером за спільним підприємством для отримання контракту на виконання робіт таким спільним підприємством, у якому організація виступає в якості учасника;

в. вимогу хабара від організації менеджером із питань закупівель або клієнтом в обмін на присудження контракту;

г. вимогу від організації збоку її клієнта щодо призначення певного субпідрядника або постачальника в обставинах, коли менеджер клієнта або державний службовець може отримати особистий зиск від такого призначення;

д. сплату хабара агентом організації менеджеру клієнтської організації від імені організації;

е. сплату хабара постачальником або субпідрядником організації на користь менеджера з питань закупівлі організації в обмін на присудження певного контракту.

A.13.1.2. Якщо організація або діловий партнер реалізувала заходи з контролю протидією хабарництву стосовно таких ризиків, подальші ризики хабарництва для організації зазвичай мінімізуються.

A.13.1.3. Вимога Статті 8.5 розрізняє організації, які контролює організація, і ті, які вона не контролює. У рамках даної вимоги вважається, що організація контролює іншу, якщо вона прямо чи опосередковано контролює управління такою організацією. Організація може мати контроль, наприклад, над філіалом, спільним підприємством або консорціумом через більшість голосів у раді правління або володіння більшістю акцій. У рамках даної вимоги вважається, що одна організація не контролює іншу лише тому, що передає їй велику частину роботи.

A.13.2. Підконтрольні організації

A.13.2.1. Організації логічно очікувати, що будь-яка інша підконтрольна їй організація реалізовує обґрунтовані й пропорційні засоби контролю протидією хабарництву. Підконтрольна організація може реалізовувати ту ж саму систему управління протидією хабарництву, що і сама організація, або ж використовувати власні засоби контролю протидією хабарництву. Слід, щоб такі засоби були обґрунтованими й пропорційними ризикам

хабарництва, із якими стикається підконтрольна організація, зважаючи на оцінку ризиків хабарництва,

яка проводилася відповідно до 4.5.

A.13.2.2. Коли організація контролює ділового партнера (наприклад, через спільне підприємство, де організація володіє управлінським контролем), такий підконтрольний партнер підпадає під вимоги 8.5.1.

A.13.3. Непідконтрольні ділові партнери

A.13.3.1. У тому випадку, коли ділові партнери непідконтрольні організації, останній можуть не знадобитися кроки, що вимагаються 8.5.2, для реалізації діловим партнером засобів контролю протидією хабарництву за наступних умов:

а. коли діловий партнер становить ризик хабарництва «низького» ступеня або взагалі не становить жодних подібних ризиків; або

б. коли діловий партнер становить ризик хабарництва зі ступенем вище «низького» але засоби контролю, які можуть вживатися діловим партнером, не допоможуть мінімізувати такий ризик (немає сенсу наполягати на вживанні діловим партнером засобів контролю, які не допоможуть; проте в даному випадку від організації очікується, що вона зважить на такий фактор протягом проведення оцінки ризиків задля того, щоб ухвалити зважене рішення стосовно того, як надалі продовжувати ділові стосунки, і чи продовжувати їх взагалі).

Це відображає обґрунтованість і пропорційність даного документу.

A.13.3.2. Якщо оцінка ризиків хабарництва (див. 4.5) або комплексна перевірка «due diligence» (див. 8.2) приходить до висновку, що непідконтрольний діловий партнер становить ризик хабарництва зі ступенем вище «низького», і що засоби контролю протидією хабарництву, які вживаються діловим партнером., можуть допомогти мінімізувати такий ризик, організації слід
перейти до подальших кроків, приведених у 8.5.

а. Організація визначає, чи оперує її діловий партнер належними засобами контролю протидією хабарництву, що відповідають чинному ризику хабарництва. Організації слід визначити це після проведення комплексної перевірки «due diligence» (див. Статтю A.10). Організація намагається перевірити, чи такі засоби контролю дозволяють упоратися з ризиком, який стосується певного правочину між організацією та діловим партнером. Організації не потрібно перевіряти, чи в ділового партнера є засоби контролю над ширшим спектром ризиків хабарництва. Слід пам'ятати про те, що масштаби засобів контролю й кроки, яких вживає організація для перевірки таких засобів контролю, мають бути обґрунтованими й пропорційними відповідному ризику хабарництва. Якщо організація визначила, допоки це вважається доцільним, що в її ділового партнера є функціонуючі засоби контролю, стосовно такого ділового партнера застосовується вимога 8.5. Дивіться Статтю A.13.3.4 для ознайомлення з коментарями з приводу відповідних типів засобів контролю.

б. Якщо організація визначає, що в ділового партнера немає функціонуючих засобів контролю протидією хабарництву для управління відповідними ризиками хабарництва, або ж коли неможливо перевірити, що такі засоби контролю функціонують, організація вживає наступних кроків:

1) У випадку практичної доцільності (див. A.13.3.3) організація вимагає від ділового партнера реалізації засобів контролю протидією хабарництву (див. A.13.3.4) стосовно відповідного правочину, проекту або діяльності.

2) У випадку відсутності практичної доцільності (див. A.13.3.3) вимагати від ділового партнера реалізації засобів контролю протидією хабарництву, організація бере цей фактор до уваги протягом оцінки ризиків хабарництва, які становить такий діловий партнер, а також спосіб, у який організація управляє такими ризиками. Це не означає, що організація не може продовжувати певні стосунки або правочини. Проте

організації в рамках оцінки ризиків хабарництва слід зважати на вірогідність причетності ділового партнера до хабарництва, і організації слід зважати на відсутність таких засобів контролю протягом загальної оцінки ризику хабарництва. Якщо організація вважає, що ризики хабарництва, які становить її діловий партнер, неприйнятно високі, і такі ризики неможливо мінімізувати іншими засобами (наприклад, шляхом реструктуризації правочину),

у такому випадку застосовуються положення Статті 8.8.

A.13.3.3. Вважається це доцільним для організації вимагати від непідконтрольних ділових партнерів реалізації засобів контролю чи ні – залежить від поточних обставин. Наприклад:

а. Зазвичай вважається практично доцільним, коли організація має значний рівень впливу на ділового партнера. Наприклад, коли організація уповноважує агента виступати від свого імені в рамках правочину або субпідрядника – в рамках значного об'єму робіт. У такому випадку організація зазвичай спроможна реалізувати засоби контролю протидією хабарництву в якості обов'язкової умови такого призначення.

б. Зазвичай не вважається практично доцільним, коли організація не має значного впливу на ділового партнера, як наприклад, на:

1) клієнта проекту;

2) певного субпідрядника або постачальника, номінованого клієнтом;

3) основного субпідрядника або постачальника, коли переговорні позиції такого субпідрядника або постачальника значно вагоміші за ті, які має організація (наприклад, коли організація закуповує в основного постачальника компоненти на стандартних умовах такого постачальника).

в. Зазвичай не вважається практично доцільним, коли діловому партнеру бракує ресурсів або робочого досвіду для реалізації таких засобів контролю.

A.13.3.4. Типи засобів контролю, які вимагаються організацією, залежать від обставин. Їх слід визначати обґрунтованими й пропорційними до ризиків хабарництва, і вони повинні включати в себе щонайменше відповідні ризики хабарництва. Залежно від природи ділового партнера та ступеня ризику хабарництва, який він становить, організація може, наприклад, вжити наступних кроків:

а. У випадку ділового партнера з високим ступенем ризику хабарництва, який займається широким спектром комплексних робіт, організація може вимагати від такого ділового партнера реалізації засобів контролю, які еквівалентні тим, що вимагаються даним документом щодо відповідних ризиків хабарництва, що їх діловий партнер становить для організації.

б. У випадку із діловим партнером середнього розміру й ризиком хабарництва «середнього» ступеня, організація може вимагати від такого ділового партнера реалізації принаймні мінімальних вимог до протидії хабарництву, які стосуються певного правочину, наприклад, політики протидії хабарництву, підготовки відповідного персоналу, уповноваження менеджера на забезпечення відповідності правочину, засобів контролю за ключовими виплатами та підзвітності.

в. У випадку з діловими партнерами невеликого розміру зі спеціалізованою сферою зайнятості (наприклад, агент або невеликий постачальник), організація може вимагати від такого партнера підготовки відповідного персоналу, а також засобів контролю над ключовими виплатами, подарунками й проявами гостинності.

Що стосується засобів контролю, їм слід працювати виключно щодо правочину між організацією й діловим партнером (хоча на практиці діловий партнер може мати засоби контролю, які застосовуються до всього бізнесу такого партнера).

Вказані вище ситуації можна використовувати виключно в якості прикладів. Важливе питання полягає в тому, щоб організація могла визначити ключові ризики хабарництва стосовно

певного правочину і наскільки це можливо – вимагати від ділового партнера реалізації обґрунтованих і пропорційних засобів контролю над такими ключовими ризиками хабарництва.

A.13.3.5. Організація зазвичай накладає такі вимоги стосовно непідконтрольних ділових партнерів у якості передумови для роботи з діловим партнером і/або в рамках документу відповідного контракту.

A.13.3.6. Від організації не вимагається проводити перевірки повної відповідності непідконтрольних ділових партнерів вказаним вимогам. Проте організації слід вжити обґрунтованих кроків щодо задоволення власних вимог до відповідності ділового партнера (наприклад, через запити до ділового партнера щодо передачі копій відповідної документації політики). У випадком з високим ступенем ризику хабарництва (наприклад, із агентом), організація може провести процедури моніторингу,

звітування і/або аудиту.

A.13.3.7. Зважаючи на те, що реалізація засобів контролю протидією хабарництву може потребувати певного часу, для організації було б доцільно дати такий час своїм діловим партнерам на реалізацію таких засобів. Організація має можливість продовжити роботу з таким діловим партнером на проміжному етапі, але подальша відсутність засобів контролю може вважатися фактором для проведення оцінки ризиків і процедури комплексної перевірки «due diligence». Проте організації також слід зважити на можливість вимагати права на розірвання певного контракту або договору, якщо діловий партнер не проводить ефективної і вчасної реалізації потрібних засобів контролю.

A.14. Зобов'язання з протидії хабарництву

A.14.1. Дана вимога щодо отримання зобов'язань із протидії хабарництву стосується виключно тих ділових партнерів, які становлять ризик хабарництва зі ступенем вище «низького».

A.14.2. Ризик хабарництва стосовно правочину, швидше за все, буде низьким у тих випадках, коли, наприклад:

а. організація закуповує незначну кількість товарів низької вартості;

б. організація бронює авіа квитки або номери в готелі через Інтернет безпосередньо в аеропортах і готелях;

в. організація постачає товари або послуги низької вартості замовнику напряму (наприклад, харчові продукти, квитки в кінотеатр).

У таких випадках від організації не вимагається отримувати зобов'язання з протидії хабарництву від постачальників із низьким ступенем ризику або замовників.

A.14.3. У випадку з діловим партнером, який становить ризик хабарництва зі ступенем вище «низького», організація, за існування такої практичної необхідності, отримує зобов'язання щодо протидії хабарництву від такого ділового партнера.

а. Зазвичай вважається доцільними вимагати таких зобов'язань, коли організація має певний вплив на ділового партнера, і коли вона може наполягти на таких зобов'язаннях від ділового партнера. Швидше за все, організація зможе отримати такі зобов'язання в тому випадку, коли вона, наприклад, уповноважує агента діяти від свого імені в рамках певного правочину, або коли обирає субпідрядника зі значним об'ємом робіт.

б. Організація може не мати достатнього впливу на ділового партнера, щоб вимагати від нього таких зобов'язань у тому випадку, коли вона, наприклад, має справу з великими клієнтами або замовниками, або коли закуповує компоненти від основного постачальника на стандартних умовах останнього. У таких випадках відсутність таких положень не означає, що проект або відносини не слід продовжувати, але до відсутності таких зобов'язань слід відноситися, як до відповідного фактору в рамках проведення

оцінки ризиків хабарництва або процедур комплексної перевірки «due diligence» відповідно до 4.5 і 8.2.

A.14.4. За існування практичної можливості такі зобов'язання слід отримувати в письмовій формі. Це може бути окремий зобов'язуючий документ або частина контракту між організацією й діловим партнером.

A.15. Подарунки, прояви гостинності, пожертви та аналогічні внески

A.15.1. Організації слід пам'ятати про те, що подарунки, прояви гостинності, пожертви та аналогічні внески можуть сприйматися третьою стороною (наприклад, діловим конкурентом, пресою, прокурором або суддею) в якості засобу для хабара, навіть якщо ані дарувальник, ані одержувач такого не планували. Корисним механізмом контролю вважається повне уникання будь-яких подарунків, проявів гостинності, пожертв та аналогічних внесків, що можуть обґрунтовано сприйматися третьою стороною, як інструмент хабарництва.

A.15.2. «Аналогічні внески», на які посилаються в 8.7, можуть включати в себе, наприклад: а.

подарунки, прояви розважальних заходів і гостинності;

б. політичні або доброчинні внески;

в. фінансування поїздок представника клієнта або державного службовця; г.

промоційні витрати;

д. спонсорство;

е. громадські переваги;

ж. тренінги;

з. клубне членство;

и. особисті послуги;

к. конфіденційна й привілейована інформація.

A.15.3. Що стосується подарунків і проявів гостинності, процедури, які реалізуються організацією, могли б, наприклад, розроблятися для:

а. контролю за об'ємом і частотою подарунків і проявів гостинності шляхом: 1) повної

заборони на отримання будь-яких подарунків і проявів гостинності; або

2) дозволу на отримання подарунків і проявів гостинності, обмежуючи їх при цьому з огляду на:

i) максимальну вартість (що може відрізнятися залежно від розташування й типу подарунку або прояву гостинності);

ii) частоту (порівняно незначні подарунки й прояви гостинності можуть у підсумку дати значну суму, якщо вони даруються достатньо часто);

iii) час (наприклад, протягом або ж одразу після переговорів щодо тендеру);

iv) обґрунтованість (зважаючи на місце розташування, сферу й старшинство дарувальника або одержувача);

v) особу одержувача (наприклад, особа, яка обіймає посаду, що дозволяє присуджувати контракти або затверджувати дозволи, сертифікати або виплати);

vi) принцип взаємності (нікому в організації не дозволяється отримувати подарунок або прояв гостинності, якщо його вартість перевищує вартість подарунку або прояву гостинності, який їм дозволяється дарувати);

vii) нормативно-правове середовище (у деяких місцях та організаціях можуть існувати заборони або певні засоби контролю);

б. вимоги попереднього затвердження подарунків або проявів гостинності відповідним керівником, якщо їх вартість або частота перевищує встановлені норми;

в. вимагати, щоб подарунки і прояви гостинності, вартість або частота яких перевищує встановлені норми, дарувалися відкрито і фіксувалися належним чином (наприклад, у реєстрі або журналі), і щоб за цим процесом було встановлено відповідний нагляд.

A.15.4. Що стосується політичних або благодійних внесків, спонсорства, промоційних витрат та громадських переваг, процедури, які реалізуються організацією, могли б, наприклад, розроблятися для:

а. заборони виплат, запланованих для здійснення впливу, або ж які можуть обґрунтовано сприйматися в якості здійснення впливу на тендер або інше рішення на користь організації;

б. проведення комплексної перевірки «due diligence» політичної партії, благодійного або іншого одержувача для визначення їх законності й відсутності можливості для їх використання в якості інструменту хабара (наприклад, це може включати в себе Інтернет-пошук або відповідні запити для того, щоб переконатися в тому, що керівники політичних партій або благодійних

організацій мають не мають репутації хабарників або аналогічної незаконної поведінки, а також чи не пов'язані вони з проектами або замовниками організації);

в. вимоги щодо затвердження виплат відповідним керівником;

г. вимоги щодо оприлюднення виплат;

д. забезпечення законності виплат відповідно до застосовного права й нормативних документів;

е. уникнення внесків одразу перед, протягом або після переговорів щодо підписання контрактів.

A.15.5. Що стосується оплати поїздок представника клієнта або державного службовця процедури, які реалізуються організацією, могли б, наприклад, розроблятися для:

а. того, щоб дозволити виключно ті виплати, які дозволяються процедурами клієнта, органу державної влади, застосовним правом і нормативними документами;

б. того, щоб дозволити виключно ті поїздки, які вважаються необхідними для належного виконання представником клієнта або державним службовцем своїх обов'язків (наприклад, інспектування системи контролю якості організації на її виробничих потужностях);

в. вимоги щодо затвердження виплат відповідним керівником організації;

г. вимоги щодо повідомлення (за існування такої можливості) начальства державного службовця, роботодавця або Підрозділу забезпечення нормативно-правової відповідності про заплановані поїздки й супутні прояви гостинності;

д. обмеження виплат до певного рівня, який вважається необхідним для здійснення поїздки, розміщення та харчування, та обґрунтовано прив'язаний до маршруту поїздки;

е. обмеження супутніх розважальних заходів до обґрунтованого рівня, як і у випадку з політикою організації щодо подарунків і проявів гостинності;

ж. заборони на компенсації витрат членів сім'ї або друзів;

з. заборони компенсації витрат у відпустці та оплати відпочинку.

МІЖНАРОДНИЙ СТАНДАРТ ISO 37001:2016(E) A.16. Внутрішній аудит

A.16.1. Вимога Статті 9.2 не означає, що організація зобов'язана мати власний окремий підрозділ для проведення внутрішнього аудиту. Вона вимагає від організації призначити придатний, компетентний і незалежний структурний підрозділ або особу, який нестиме відповідальність за проведення такого аудиту. Організація може скористатися послугами третьої сторони для проведення всієї програми внутрішнього аудиту або ж залучити третю сторону для реалізації лише певних частин чинної програми.

A.16.2. Частота проведення аудиту залежатиме від вимог організації. Швидше за все, для проведення аудиту щороку визначатиметься певна вибірка проектів, контактів, процедур, засобів контролю та систем.

A.16.3. Визначення такої вибірки може базуватися на ризиках, щоб, наприклад, проект із високим ступенем ризику хабарництва ставав би пріоритетом для аудиту у порівнянні з проектом із низьким ступенем ризику хабарництва.

A.16.4. Зазвичай аудити плануються заздалегідь, щоб відповідні сторони встигли підготувати потрібну документацію й виділили на таку роботу певний час. Проте в окремих випадках організація може вважати за корисне провести неочікуваний аудит для відповідних його учасників.

A.16.5. Якщо в організації є керівний орган, він також може спрямовувати процес вибірки та частоту проведення аудитів у організації, як він це вважає за потрібне, щоб забезпечити незалежність і досягнення цілей аудиту в основних зонах ризику хабарництва організації. Керівний орган також може мати доступ до всіх аудиторських звітів та відповідних результатів, а також забезпечити, щоб будь-які результати аудиту, що виявляють певні типи підвищеного ризику хабарництва або відповідні індикатори повідомлялися керівному органу після завершення аудиту.

A.16.6. Наміром аудиту вважається обґрунтоване переконання керівного органу (якщо такий є) і вищого керівництва організації в реалізації й ефективному функціонуванні системи управління

протидією хабарництву, допомога із запобіганням і виявленням випадків хабарництва, а також стримуючі засоби для будь-якого потенційно корумпованого персоналу (адже вони знатимуть, що їх проект або департамент було обрано для аудиту).

A.17. Задокументована інформація

За визначенням 7.5.1 задокументована інформація може включати в себе: а.

доведення політики протидії хабарництву до персоналу;

б. доведення політики протидії хабарництву до ділових партнерів, які становлять ризик хабарництва зі ступенем вище «низького»;

в. політику, процедури й засоби контролю системи управління протидією хабарництву; г.

результати оцінки ризиків хабарництва (див. 4.5);

д. проведені тренінги з протидії хабарництву (див. 7.3);

е. проведене комплексна перевірка «due diligence» (див. 8.2);

ж. вжиті заходи для реалізації системи управління протидією хабарництву;

з. затвердження й записи про подарунки, прояви гостинності, пожертви й аналогічні внески, одержані й даровані (див. 8.7);

и. заходи й результати перевірки повідомлень стосовно:

1) будь-яких недоліків системи управління протидією хабарництву;

 2) випадків спроби, підозри або реального хабарництва;

к. результати моніторингу, розслідування або аудиту, що проводився організацією або третіми сторонами.

A.18. Розслідування та вирішення проблем хабарництва

A.18.1. Даним документом від організації вимагається реалізувати належні процедури з приводу методів ведення розслідування й вирішення проблеми хабарництва або порушення вимог засобів контролю протидією хабарництву, про які повідомляють, які фіксують або обґрунтовано підозрюють. Методи ведення розслідування й вирішення конкретних випадків залежатимуть від обставин. Кожна ситуація унікальна, і реакція організації на таку ситуацію має бути обґрунтованою й пропорційною до обставин. Повідомлення або звіт про підозру щодо серйозного випадку хабарництва може потребувати термінових, масштабних і детальних дій у порівнянні з незначним порушенням вимог засобів контролю протидією хабарництву. Вказані нижче приклади приведено виключно з інформаційною метою, і їх не слід сприймати в якості інструкцій до виконання.

A.18.2. Бажаним адресатом усіх повідомлень про підозру або реальний випадок хабарництва чи порушення вимог засобів контролю протидією хабарництву слід призначити Підрозділ забезпечення нормативно-правової відповідності. Якщо в якості першої інстанції виступає інша особа, процедури організації мали б вимагати подальшої передачі такого звіту Підрозділу забезпечення нормативно-правової відповідності якнайшвидше. У деяких випадках Підрозділ забезпечення нормативно-правової відповідності може самостійно виявляти підозри або порушення.

A.18.3. Процедурою слід визначити відповідальність за ухвалення рішень стосовно методу ведення розслідування та вирішення проблеми. Наприклад:

а. невеличка організація може мати процедуру, за якою всі питання, не зважаючи на їх серйозність, повідомляються Підрозділом забезпечення нормативно-правової відповідності безпосередньо вищому керівництву для ухвалення управлінського рішення стосовно майбутнього реагування на такий випадок;

б. більша організація може мати процедуру, відповідно до якої:

1) незначні проблеми вирішуються Підрозділом забезпечення нормативно-правової відповідності, який подає регулярні звіти про всі такі проблеми вищому керівництву;

2) значні проблеми негайно доводяться Підрозділом забезпечення нормативно-правової

відповідності безпосередньо до вищого керівництва для ухвалення управлінського рішення стосовно майбутнього реагування на такий випадок.

A.18.4. У випадку виявлення будь-якої проблеми, вищому керівництву або Підрозділу забезпечення нормативно-правової відповідності (за існування такої необхідності) слід оцінити відомі факти й потенційну серйозність проблеми. Якщо в них ще не має достатніх фактів для ухвалення рішення, їм слід ініціювати відповідне розслідування.

A.18.5. Розслідування слід доручити особі, яка не була причетна до відповідної проблеми. Це може бути Підрозділ забезпечення нормативно-правової відповідності, структурний підрозділ внутрішнього аудиту, відповідний керівник або третя сторона. Особу, яка займається розслідуванням, слід забезпечити відповідними повноваженнями, ресурсами й доступом до вищого керівництва для ефективного провадження слідчих дій. Бажано, щоб особа, яка займається розслідуванням, пройшла відповідну підготовку або мала попередній досвід із ведення слідчих дій. Протягом розслідування слід оперативно встановити факти та зібрати необхідні докази, наприклад, шляхом:

а. запитів для встановлення фактів;

б. збору всієї необхідної документації та інших доказів;

 в. отримання показів свідків;

г. коли це можливо й доцільно, запитів щодо отримання звітів про відповідне питання в письмовій формі та за підписом фізичних осіб, які такі звіти готують.

A.18.6. Протягом розслідування й будь-яких подальших дій організації потрібно зважати на відповідні фактори, як наприклад:

а. застосовне право (може знадобитися відповідна правова допомога);

б. безпека персоналу;

в. ризик дискредитації від певних заяв;

г. захист осіб, які подають повідомлення (звіти), та інших осіб, які причетні, або на яких посилаються у звіті (див. 8.9);

д. потенційна кримінальна, цивільна й адміністративна відповідальність, фінансові збитки та шкода для репутації для організації й окремих осіб;

е. будь-які правові зобов'язання чи переваги для організації, про які слід повідомити органи влади;

ж. дотримання таємниці слідства до встановлення реальних фактів;

з. необхідність для вищого керівництва вимагати повної співпраці протягом слідства від відповідного персоналу.

A.18.7. Про результати розслідування слід повідомляти вище керівництво або Підрозділ забезпечення нормативно-правової відповідності в разі такої необхідності. Якщо про результати повідомляють вище керівництво, їх також слід доводити до відома Підрозділу забезпечення нормативно-правової відповідності.

A.18.8. Щойно організація завершує розслідування, і/або має достатньо інформації, щоб ухвалити відповідне рішення, організації слід вжити відповідних подальших заходів. Залежно від обставин й серйозності проблеми, такі заходи можуть включати в себе наступне:

а. припинення, вихід або зміна рівня участі організації в проекті, правочині або контракті; б.

компенсація або повернення будь-якої неправомірно отриманої вигоди;

в. дисциплінарне покарання для відповідного персоналу (яке залежно від серйозності проблеми може бути попередженням – для незначного порушення або ж звільненням – для серйозного проступку);

г. повідомлення про проблему органів влади;

д. у випадку реального хабара, вжиття заходів для уникнення або вирішення будь-яких можливих наступних правопорушень (наприклад, у випадку невірного визначення хабара в бухгалтерській звітності може статися фальсифікація бухгалтерії; у випадку невірного віднімання суми хабара

від отриманого прибутку може статися податкове правопорушення; а у випадку з коштами, отриманими незаконним шляхом, може статися відмивання грошей).

A.18.9. Організації слід переглядати свої процедури з протидії хабарництву, щоб перевірити, чи не виникла певна проблема через певні невідповідності в чинних процедурах, і чи не потрібно вжити належних заходів для вдосконалення чинних процедур.

A.19. Моніторинг

Моніторинг системи управління протидією хабарництву може включати в себе, наприклад, наступні сфери:

 а. ефективність підготовки (тренінгів);

б. ефективність засобів контролю, наприклад, шляхом вибірки результатів тестів;

в. ефективність розподілу обов'язків для відповідності вимогам системи управління протидією хабарництву;

г. ефективність вирішення попередньо виявлених проблем з відповідністю; д.

випадки не проведення запланованих внутрішніх аудитів.

Моніторинг відповідності виконання може включати в себе, наприклад, наступні сфери: —

невідповідність і «промашки» (випадок, що не мав негативного впливу); — випадки

невиконання вимог протидії хабарництву;

— випадки недосягнення поставлених цілей;

— стан культури відповідності.

ПРИМІТКА: Дивіться Стандарт ISO 19600.

Організація може проводити періодичну самооцінку всієї організації або її частин для оцінки ефективності системи управління протидією хабарництву (див. 9.4).

A.20. Планування й запровадження змін до системи управління протидією хабарництву

A.20.1. Адекватність та ефективність системи управління протидією хабарництву слід оцінювати на постійній і регулярній основі кількома методами, як наприклад, аналіз шляхом внутрішнього аудиту (див. 9.2), аналізу збоку керівництва (див. 9.3) та збоку Підрозділу забезпечення нормативно-правової відповідності (див. 9.4).

A.20.2. Організації слід зважати на результати й продукти таких оцінок для визначення ймовірності потреби або можливості для зміни системи управління протидією хабарництву.

A.20.3. Для забезпечення виконання вимог щодо цілісності й ефективності системи управління протидією хабарництву, зміни окремих складових системи управління повинні брати до уваги залежність і вплив таких змін на ефективність роботи системи управління в цілому.

A.20.4. Коли організація визначає потребу в зміні системи управління протидією хабарництву, такі зміни слід проводити планово і зважаючи на наступне:

а. мету змін і їх потенційні наслідки;

б. цілісність системи управління протидією хабарництву;

в. доступність ресурсів;

г. розподіл або перерозподіл відповідальності й повноважень;

д. рівень, масштаби й графік проведення змін.

A.20.5. Удосконалення системи управління протидією хабарництву у результаті заходів, які вживаються в якості реагування на будь-які випадки невідповідності (див. 10.1) та ті, що

отримуються протягом постійного вдосконалення системи (див. 10.2), слід проводити в рамках підходу, вказаного в Статті A.20.4 вище.

МІЖНАРОДНИЙ СТАНДАРТ ISO 37001:2016(E) A.21. Державні службовці

Термін «державний службовець» (див. 3.27) широко тлумачиться в багатьох антикорупційних законах.

Нижче приведено список, який не слід вважати вичерпним, і не всі вказані приклади застосовні для всіх існуючих юрисдикцій. Протягом оцінки ризиків хабарництва організаціям слід зважати на категорії державних службовців, з якими вони мають або можуть мати справу.

Термін «державний службовець» може включати в себе наступне:

a. особи, які займають державну посаду національного, регіонального або місцевого рівня, включаючи членів законодавчих органів, осіб на адміністративних посадах і працівників системи правосуддя;

б. посадові особи політичних партій;

в. кандидати на державні посади;

г. працівники уряду, включаючи працівників міністерств, урядових агенцій, адміністративних трибуналів і державних рад;

д. посадові особи міжнародних організацій, наприклад, Світового Банку, ООН та Міжнародного Валютного Фонду;

е. працівники державних підприємств за виключенням тих випадків, коли підприємство працює на звичайних комерційних засадах відповідного ринку, тобто на засадах, аналогічних до приватного підприємства, без преференційних субсидій або інших привілеїв (див. [17] у Бібліографії).

У багатьох юрисдикціях родичі й близькі особи державних службовців у рамках антикорупційного законодавства самі вважаються державними службовцями.

A.22. Ініціативи з протидії хабарництву

Хоча це не вважається вимогою даного документу, організація може вважати за корисне долучитися або розглянути рекомендації будь-яких секторальних чи інших ініціатив протидії хабарництву, які просувають або публікують положення належної практики протидії хабарництву, що можуть стосуватися діяльності організації.

МІЖНАРОДНИЙ СТАНДАРТ ISO 37001:2016(E) Бібліографія

[1] ISO 9000, *Quality management systems — Fundamentals and vocabulary [2]*

ISO 9001, *Quality management systems — Requirements*

[3] ISO 19011, *Guidelines for auditing management systems*

[4] ISO 14001, *Environmental management systems — Requirements with guidance for use [5]*

ISO/IEC 17000, *Conformity assessment — Vocabulary and general principles [6]* ISO 19600,

Compliance management systems — Guidelines

[7] ISO 22000, *Food safety management systems — Requirements for any organization in the food chain*

[8] ISO 26000, *Guidance on social responsibility*

[9] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[10] ISO 31000, *Risk management — Principles and guidelines*

[11] ISO Guide 73, *Risk management — Vocabulary*

[12] ISO/IEC Guide 2, *Standardization and related activities — General vocabulary*

[13] BS 10500, *Specification for an системи управління протидією хабарництву*

[14] United Nations Convention against Corruption, New York, 2004. Available at: http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

[15] Organization for Economic Co-operation and Development, Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents,

Paris, 2010

[16] Organization for Economic Co-operation and Development, Good Practice Guidance on Internal Controls, Ethics, and Compliance, Paris, 2010

[17] Organization for Economic Co-operation and Development, Commentaries on the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, 21 November 1997

[18] United Nations Global Compact/Transparency International, Reporting guidance on the 10th

principle against corruption, 2009

[19] International Chamber of Commerce, Transparency International, United Nations Global Compact and World Economic Forum, RESIST: Resisting Extortion and Solicitation in International Transactions, A company tool for employee training, 2010

[20] International Chamber of Commerce, Rules on Combating Corruption, Paris, 2011 [21]

Transparency International, Business Principles for Countering Bribery and associated tools,

Berlin, 2013

 [22] Transparency International,

Corruption Perceptions Index

[23] Transparency International, Bribe Payers Index

[24] World Bank, Worldwide Governance Indicators Bank

[25] International Corporate Governance Network, ICGN Statement and Guidance on Anti Corruption Practices, London, 2009

[26] World Economic Forum, Partnering Against Corruption Principles for Countering Bribery, An Initiative of the World Economic Forum in Partnership with Transparency International and the Basel Institute on Governance, Geneva

[27] Committee of the Sponsoring Organizations of the Treadway Commission (COSO): Internal Control – Integrated Framework, May 2013

ICS 03.100.01

Ціна 47 сторінок

© ISO 2016 – Усі права зберігаються