Т Р Е Н І Н Г

Впровадження системи внутрішнього контролю в державному секторі:
ВИМОГИ та КРАЩІ ПРАКТИКИ

1-й день 3-тя тема

КОМПЛАЄНС

(контроль за дотриманням вимог, у т.ч. щодо вірогідності виникнення конфлікту інтересів та за інформаційною безпекою і обміном інформацією)

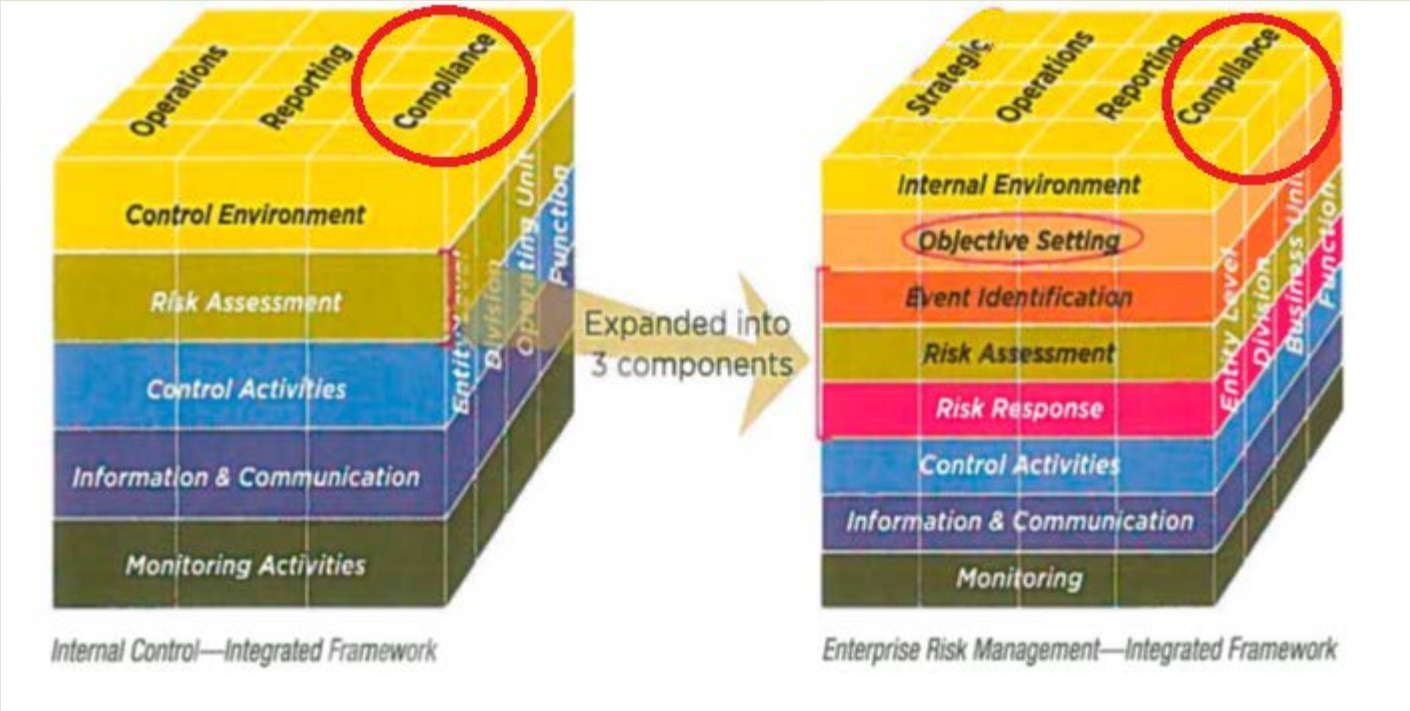
м. Київ

13 - 17 березня 2017

КОНСУЛЬТАНТ

Лебединець Тетяна Леонідівна
Президент Правління Інституту
внутрішніх аудиторів України
Телефон: +38(050)377 -11-97,
+38(050)418-88-11
E-mail: lebedynets.tl@gmail.com,
tatyana.lebedynets@iia.org.ua

Інтегрована модель COSO – Управління ризиками організації



The Institute of Internal Auditors

Концепція COSO поділяє цілі організації на три категорії: операційні, цілі в області звітності та **комплаєнс**.

Визначення внутрішнього контролю відповідно до COSO говорить що – це **процес, який призначений забезпечити достатню впевненість у виконанні цілей** операційної діяльності, звітності та **комплаєнсу**.

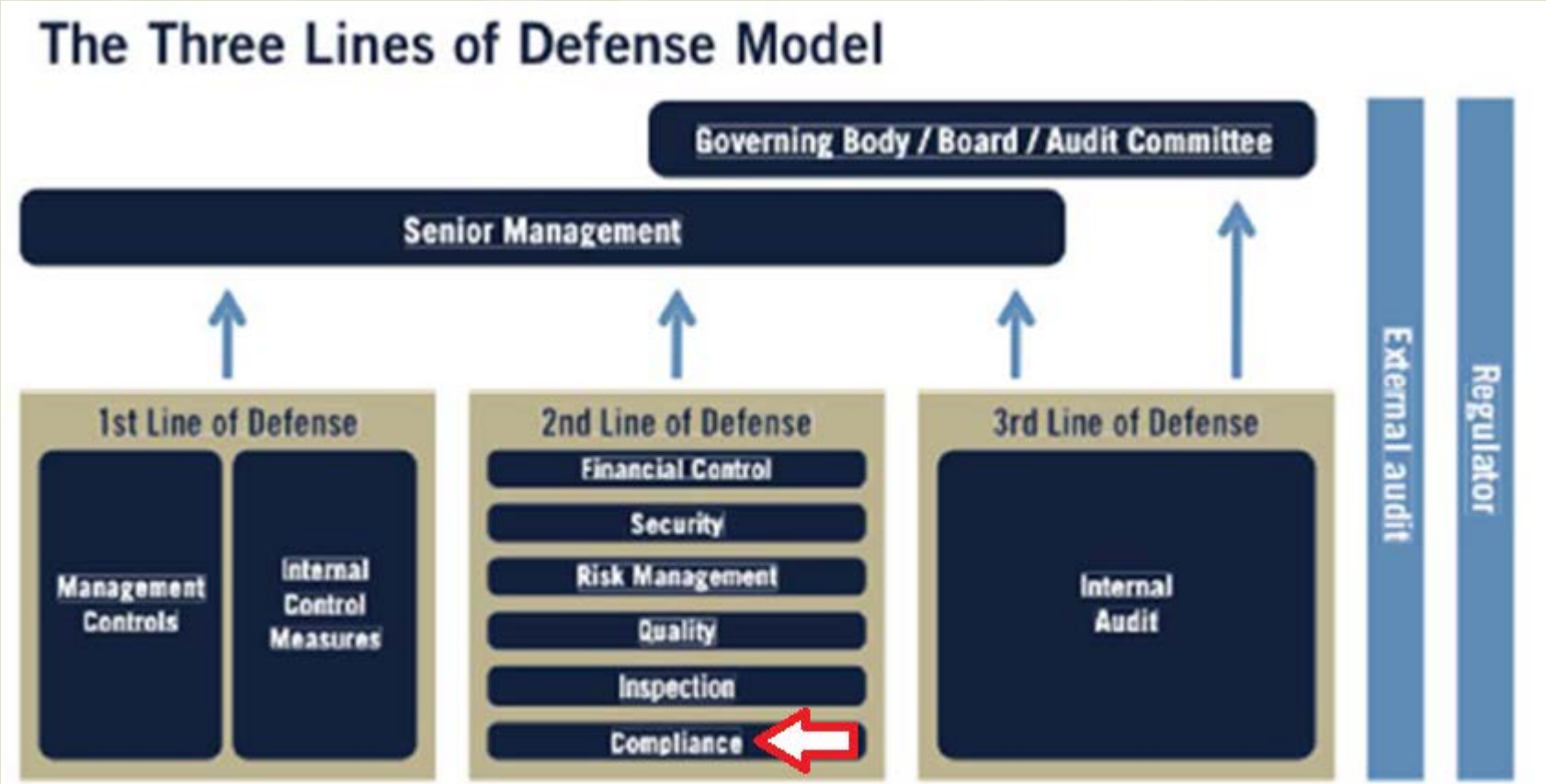
Комплаєнс відповідно до словника COSO - це відповідність вимогам законів та нормативних актів, які властиві діяльності юридичні організації.

В той самий час COSO говорить, що організація може визначити декілька під цілей для кожного виду діяльності, виходячи з цілей рівня організації та встановлених стандартів, пов'язаних з цілями в області дотримання законодавства та підготовки звітності, залежно від конкретної ситуації. Наприклад, операційні цілі функції закупівель можуть включати в себе:

- закупівля товарів у відповідності до технічних специфікацій;
- закупівля товарів у компаній, які відповідають вимогам екології, охорони праці та техніки безпеки (наприклад, без залучення дитячої праці, хороші умови роботи)
- введення переговорів відповідно до прийнятної ціни та інших умов.

Ще один приклад, керівництво може поставити наступну ціль в області підготовки зовнішньої фінансової звітності на рівні організації: «Наша організація готує достовірну фінансову звітність, відображаючи операції та події у відповідності о загальноприйнятих стандартів звітності».

Модель трьох ліній захисту
розроблена Інститутом внутрішніх аудиторів



Graph 1: The Three Lines of Defense Model (IIA (2013))

The Institute of Internal Auditors


КОМПЛАЄНС
Подарунки
Дозволи та ліцензії
Державна таємниця/конференційна інформація
Послуги та процеси
Етика та поведінка
Закупівлі
Інсайдерська інформація
Конфлікт інтересів
Регуляторні органи
Маркетинг та реклама
Робота поза офісом
Обслуговування клієнтів

Чим займається комплаєнс у своїй щоденній діяльності?

Конфлікт інтересів

26 квітня 2015 року введений в дію Закон України "Про запобігання корупції" від 14.10.2014 № 1700-VII (далі – Закон № 1700), який значно детальніше, ніж попередній антикорупційний закон «Про засади запобігання і протидії корупції» від 07.04.2011 № 3206-VI (далі – Закон № 3206), регламентує питання, пов'язані з конфліктом інтересів на публічній службі та його врегулюванням.

Норми Закону № 1700 щодо запобігання та врегулювання конфлікту інтересів поширюються на осіб, зазначених у пунктах 1, 2 частини першої статті 3 цього Закону, тобто на осіб, уповноважених на **виконання функцій держави або місцевого самоврядування та на прирівняних до них осіб**.

Конфлікт інтересів

Конфлікт інтересів можливий реальний або потенційний. Згідно зі ст. 1 Закону України «Про запобігання корупції» (далі – Закон), потенційний конфлікт інтересів – це **наявність у особи приватного інтересу у сфері**, в якій вона виконує свої службові чи представницькі повноваження, що **може вплинути на об'єктивність чи неупередженість прийняття нею рішень,** або на вчинення чи невчинення дій під час виконання зазначених повноважень. Реальний конфлікт інтересів – це **суперечність між приватним інтересом особи та її службовими чи представницькими повноваженнями**, що впливає на об'єктивність або неупередженість прийняття рішень, або на вчинення чи невчинення дій під час виконання зазначених повноважень.

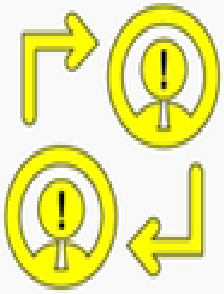
Приватний інтерес – це **будь-який майновий чи немайновий інтерес особи**, у тому числі зумовлений особистими, сімейними, дружніми чи іншими позаслужбовими стосунками з фізичними чи юридичними особами, у тому числі ті, що виникають у зв'язку з членством або діяльністю в громадських, політичних, релігійних чи інших організаціях.

Конфлікт інтересів на державній службі

Конфлікт інтересів – суперечність між приватним інтересом особи та її службовими чи представницькими повноваженнями, що впливає на об'єктивність або неупередженість прийняття особою рішень чи вчинення дій під час виконання повноважень.

Види конфлікту інтересів:

потенційний



може потенційно виникнути суперечність

реальний

суперечність відбувається в дійсності

Недопущення виникнення конфлікту інтересів

1. Нормативні документи організації визначають контролі за недопущенням виникнення або потенційного конфлікту між особистими (приватними) інтересами та посадовими чи професійними обов'язками особи або конфлікт, що виникає під час виконання такою особою несумісних обов'язків.
2. На практиці впроваджено (мінімальні вимоги).
3. Працівники організації при прийомі на роботу заповнюють форму про наявність/відсутність конфлікту інтересів. Форми оновлюються на регулярній основі (обов’язково при виникненні ризику).
4. Підрозділ/особа, відповідальний за комплаєнс на регулярній основі здійснює моніторинг діяльності працівників та керівництва організації на предмет наявності/відсутності конфлікту інтересів (прийняття цінних подарунків, використання власності організації в особистих цілях, використання або розкриття конфіденційної інформації, наявність економічної або фінансової заінтересованості в діяльності постачальників, клієнтів, заінтересованих осіб або конкурентів організації, прямого підпорядкування та залежності пов’язаних працівників).
5. Організація виявляє та контролює пов’язаність клієнтів та контрагентів.

Недопущення виникнення конфлікту інтересів

На практиці необхідно впровадити (мінімальні вимоги):

Розподіл повноважень та обов’язків має бути здійснений керівництвом чітко та з визначенням конкретних лімітів, повноважень, обмежень з метою уникнення конфлікту інтересів, шахрайств під час здійснення діяльності, виконання функцій одноосібно, або одним підрозділом (операції з рахунками клієнтів, їх відображення у бухг. обліку; прийняття рішення, моніторинг/супроводження, формування управлінської, фінансової звітності та звітності контролюючим органам).

Посадова інструкція має бути розроблена для всіх категорій працівників та чітко визначати всі функції, обов'язки, відповідальність згідно покладених завдань. Всі працівники мають бути ознайомлені під підпис зі своїми посадовими інструкціями, наказами.

Контроль за вірогідністю виникнення конфлікту інтересів

1. Наявність зобовязання працівника щодо збереження державної таємниці/конфеденційної інформації (з обмеженим доступом) при прийнятті на роботу.
2. У договорах наявне застереження щодо збереження таємниці та відповідальність за розголошення.
3. Розроблені процедури та порядок надання доступу до таємниці за використанням.
4. Встановлені та затверджені порядки ведення діловодства таємниці, відправлення, отримання та зберігання та особливості роботи з таємницею на електронних носіях.
5. Наявність та порядок ведення журналу реєстрації таємниці.
6. Відповідність оформлення запитів на розкриття таємниці. Правомірність виконання вимог та рішень відповідних органів/осіб про розкриття таємниці /надання документів, що містять таємницю.
7. Дотримання встановленого порядку передачі інформації таємниці третім сторонам або розповсюдження у СМІ, інших ресурсах(за наявності письмової згоди клієнта).
8. Відповідність автоматизованих систем, які оброблюють інформацію у частині запобігання несанкціонованому доступу.

В ході проведення розслідувань та у разі залучення фахівців ВА чи ВК

Необхідно перевірити дотримання основних принципів комплаєнс та конфіденційності:

- Працівник, який підозрюється у шахрайстві, його прямий або не прямий керівник/супервізор не можуть приймати учать у розслідуванні/перевірці;
- Керівником перевірки не може бути працівник (його родич) підрозділу, у якому виник ризик;
- Спеціальна перевірка не може проводитись одноосібно (принцип 4х очей);
- До підтвердження факту шахрайства цілі перевірки не розголошуються (відомо тільки органу, який ініціював перевірку, безпосередньому керівнику підрозділу, у якому виник ризик, учасникам команди та менеджеру з протидії шахрайству);
- Внутрішні аудитори/контролери у якості учасника спец. перевірки не приймає жодну з сторін, складає свою власну думку. Якщо думка аудитора /контролера відмінна від висновку керівника перевірки, аудитор /контролер має право надати свій власний висновок щодо інциденту.

Інформація та інформаційний обмін

Відповідно до Концепції розвитку державного внутрішнього фінансового конролю та затвердження плану заходів щодо її реалізації на період до 2017 року одним із елементів структури внутрішнього контролю є інформація та інформаційний обмін.

Інформація повинна реєструватися і надаватися керівництву та іншим користувачам органів державного і комунального сектору в такій формі і в такий час, щоб вона могла служити основою для належного виконання функцій внутрішнього контролю, внутрішнього аудиту та інших шляхом створення адекватної сучасним умовам інформційно-комунікаційної інфраструктури в системі органів державного і комунального секторру.

Контроль за інформаційною безпекою та обміном інформації

У внутрішніх документах організації мають бути визначені усі вимоги, відповідно до стандартів з управління інформаціною безпекою.

Процедури та контролі для забезпечення високого рівня управління доступами, безпекою функціонування та комунікації, засобами криптографії, інформацією з обмеженим доступом мають бути впроваджені.

Контроль за інформаційною безпекою та обміном інформації

Державні вимоги до побудови захисту інформації викладені КСЗІ (комплексна система захисту інформації), які в більшій мірі сфокусовані до захисту самих інфо систем (hard ware). Розроблені Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку). Покриваються наступні основні питання:

- захист інформації
- управління доступів
- шифрування даних
- документування
- захист мережі

ISO 2700.1 Міжнародні стандарти (більш ширші ніж КСЗІ), виходять за межі лише ІТ та охоплюють діяльність усієї організації. З 01.01.2017 року вони перекладені українською та прийняті як державні (ДСТУ (Наказ ДП «УкрНДНЦ» від 18.12.2015 №193)). В питаннях захисту ІТ систем КСЗІ і ISO 2700.1 мають схожі вимоги.

Контроль за інформаційною безпекою та обміном інформації

Практики щодо управління IT :

- COBIT - стандарт організації управління IT на підприємстві (для керівництва та внутрішнього аудиту);
- ITIL – набір найкращих практик для виконавців (технічна бібліотека), нею користуються усі компанії;
- BSI - IT-Grundschutz-Kataloge – каталог кращих практик організації інформаційної безпеки, доступний англійською та німецькою.

Контроль за інформаційною безпекою та обміном інформації

Організація здійснює котроль за обміном інформацією шляхом:

1) забезпечення адекватної, усебічної, цілісної, надійної, доступної, конфіденційної та своєчасної внутрішньої фінансової, операційної та статистичної інформації, інформації про дотримання вимог законодавства України, внутрішніх документів банку, ринкової інформації, необхідної для прийняття рішень і виконання службових обов'язків;

2) установлення порядку доведення інформації, обміну інформацією, який би забезпечував повне розуміння та дотримання працівниками організації внутрішніх політик та процедур;

3) Організація визначає форму надання інформації з урахуванням потреб та вимог конкретного користувача (органів управління, структурних підрозділів, працівників, наглядових органів, учасників та клієнтів).

Контроль за інформаційною безпекою та обміном інформації

4) Організація запроваджує ефективний обмін інформацією за різними напрямами, а саме:

1) вертикально (знизу - вгору), щоб керівництво знало і усвідомлювало ризики, на які наражається організація, та адекватно реагували, організовували та контролювали роботу;

2) вертикально (зверху - вниз), щоб інформація про стратегію та політику організації доводилася до відома всіх управлінських рівнів та інших працівників, яких залучено до управління інформаційною безпекою та обміном інформацією;

3) горизонтально, щоб інформація, якою володіє один підрозділ, надавалась іншому підрозділу, якому вона необхідна для виконання своїх функцій.

Запитання?

Дякую за увагу!