



МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

НАКАЗ

Департаменту внутрішнього аудиту Міністерства оборони України

06.10.2017

м. Київ

№ 33

Про затвердження Тимчасової настанови з
проведення аудиту управління ризиками

Відповідно до статті 26 Бюджетного кодексу України, пункту 1.2 глави 1 розділу 2 Стандартів внутрішнього аудиту, затверджених наказом Міністерства фінансів України від 04.10.2011 № 1247, зареєстрованих в Міністерстві юстиції України 20.10.2011 за № 1219/19957 (зі змінами), пунктів 4.13, 9.12 Положення про Департамент внутрішнього аудиту Міністерства оборони України, затвердженого наказом Міністерства оборони України від 24.05.2016 № 275 (зі змінами), та з метою визначення єдиного комплексу дій з проведення аудиту управління ризиками підрозділами Служби внутрішнього аудиту Збройних Сил України

НАКАЗУЮ:

1. Затвердити Тимчасову настанову з проведення аудиту управління ризиками, що додається.
2. Заступникам директора, керівникам структурних підрозділів Департаменту внутрішнього аудиту Міноборони (далі – Департамент) та територіальних управлінь внутрішнього аудиту забезпечити вивчення та застосування цієї Тимчасової настанови.
3. Наказ довести до особового складу Департаменту та територіальних управлінь внутрішнього аудиту.
4. Контроль за виконанням наказу покласти на заступника директора Департаменту – начальника відділу аудиту у сфері фінансового забезпечення.

Директор Департаменту

М.В.БАРИНІНА

ПОГОДЖЕНО:

Заступник директора Департаменту –
начальник відділу
полковник

С.В.КИРИЧЕНКО

Начальник відділу організації та
забезпечення якості внутрішнього аудиту

Ю.А.ТИЩЕНКО

Начальник Територіального управління
внутрішнього аудиту військових частин,
безпосередньо підпорядкованих
Міністерству оборони України та
Генеральному штабу Збройних Сил України
полковник

О.І.ТИТКОВСЬКИЙ

ЗАТВЕРДЖЕНО
наказ Департаменту внутрішнього аудиту
Міністерства оборони України
від _____.10.2017 № _____

ТИМЧАСОВА НАСТАНОВА
з проведення аудиту управління ризиками

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Тимчасову настанову з проведення аудиту управління ризиками (далі – Настанова) розроблено відповідно до статті 26 Бюджетного кодексу України, пункту 1.2 глави 1 розділу 2 Стандартів внутрішнього аудиту, затверджених наказом Міністерства фінансів України від 04.10.2011 № 1247, зареєстрованих в Міністерстві юстиції України 20.10.2011 за № 1219/19957 (зі змінами), пунктів 4.13, 9.12 Положення про Департамент внутрішнього аудиту Міністерства оборони України, затвердженого наказом Міністерства оборони України від 24.05.2016 № 275 (зі змінами), з метою:

визначення єдиного комплексу дій з проведення підрозділами Служби внутрішнього аудиту Збройних Сил України (далі – Служба) аудиту управління ризиками;

надання аудиторам методологічних та практичних рекомендацій з проведення аудиту управління ризиками.

1.2. Терміни, поняття, категорії та скорочення, що використовуються у цій Настанові, вживаються у значеннях, наведених у Бюджетному кодексі України, інших нормативно-правових актах, що регламентують бюджетні відносини, Положенні про Департамент внутрішнього аудиту Міністерства оборони України, Стандартах внутрішнього контролю в Міністерстві оборони України та Збройних Силах України, затверджених Міністром оборони України 4 липня 2016 року (далі – Стандарти внутрішнього контролю в Міноборони та ЗСУ), та Інструкції з організації внутрішнього контролю у Збройних Силах України, затвердженої наказом Генерального штабу Збройних Сил України від 29.08.2016 № 340 (далі – Інструкція № 340).

1.3. У процесі проведення аудиту управління ризиками (далі – аудит) посадові особи Служби повинні дотримуватися морально-етичних принципів професійної діяльності, викладених у Кодексі етики, зокрема, принципів сумлінності (цілісності, добросовісності), незалежності та об'єктивності, конфіденційності та професійної компетентності, не допускати виникнення конфлікту інтересів, а у разі його виникнення – вживати вичерпних заходів щодо врегулювання конфлікту інтересів.

1.4. Аудитори, які проводить аудит, повинні мати навички проведення системного аналізу, написання звітів зі складних питань, що вимагають логічного і ретельного обґрунтованого викладення.

1.5. Керівник та члени аудиторської групи (аудитор) виконують функції та мають права, визначені Положенням про Департамент (положеннях про територіальні підрозділи) та Порядком проведення внутрішнього аудиту підрозділами Служби.

1.6. До проведення аудиту можуть залучатися фахівці інших структурних підрозділів Міноборони, Генерального штабу, інших підконтрольних суб'єктів (за згодою їх керівників), оскільки в окремих випадках їх кваліфікація та компетентність у специфічних питаннях різних ризикових сфер діяльності дозволяють зробити відповідні висновки та допомагають підготувати аудиторський звіт належної якості і обґрунтовані рекомендації. Питання щодо залучення до аудиту таких фахівців, залежно від конкретних обставин, вирішує керівник підрозділу Служби з направленням відповідного звернення. Залучені фахівці з питань, які належать до їх повноважень, надають письмові довідки для їх використання при складанні аудиторського звіту.

II. МЕТА, ОСНОВНІ ЗАВДАННЯ ТА МЕТОДИ АУДИТУ

2.1. Метою аудиту є надання об'єктивних, обґрунтованих і незалежних рекомендацій, спрямованих на удосконалення і підвищення ефективності системи управління ризиками підконтрольного суб'єкта.

2.2. Основними завданнями аудиту є:

отримання і оцінка об'єктивних даних про місію (мету) і цілі підконтрольного суб'єкта, ризикові сфери діяльності, процеси та операції, стан організації системи управління ризиками;

дослідження, аналіз та оцінки функціонування системи управління ризиками;

надання об'єктивних, обґрунтованих і незалежних рекомендацій щодо удосконалення і підвищення ефективності системи управління ризиками.

2.3. Предметом аудиту є система управління ризиками.

Цикл управління ризиками складається з:

ідентифікації потенційних подій, що можуть вплинути на досягнення мети і цілей;

оцінки ідентифікованих ризиків;

визначення способів реагування на ризики;

розробки і затвердження заходів контролю, спрямованих на запобігання ризикам або зменшення їх негативного впливу на досягнення мети та стратегічних цілей (із доведенням затвердженого плану управління ризиками чи іншого аналогічного документа до виконавців);

постійного виконання заходів контролю із забезпеченням документального підтвердження фактів їх виконання (“аудиторський слід”);

постійного обміну інформацією та здійснення комунікацій з відповідних питань;

постійного моніторингу з боку відповідних керівників повноти виконання заходів контролю та їх ефективності;

періодичних оцінок/самооцінок системи управління ризиками та виконання наданих за їх результатами рекомендацій;

періодичного перегляду системи управління ризиками (починаючи з ідентифікації подій).

2.4. Аудит може проводитися як окремий аудит або як дослідження одного з питань (пунктів) програми в рамках іншого аудиту.

Залежно від конкретної мети, аудит управління ризиками може проводитися як:

аудит відповідності – якщо досліджуватимуться питання дотримання законодавства, виконання планів, доручень керівництва Міноборони та Генерального штабу щодо впровадження Стандартів внутрішнього контролю в Міноборони та ЗСУ, Інструкції № 340, інших нормативно-правових актів і документів;

фінансовий аудит – переважно якщо досліджуватимуться питання управління фінансовими ризиками;

аудит ефективності – якщо досліджуватимуться питання ефективності системи управління ризиками. Під час проведення такого аудиту можуть досліджуватися як одночасно економічність, продуктивність/ефективність та результативність(три “Е”¹), так і окремо одна з трьох “Е” або дві з трьох “Е”;

змішаний – якщо досліджуються питання, що належать до двох з трьох наведених вище аудитів (наприклад, аудит відповідності та фінансовий або фінансовий аудит та аудит ефективності);

комплексний – якщо одночасно проводиться аудит відповідності, фінансовий та ефективності.

Залежно від масштабу та початкових обмежень, аудит може охоплювати як всю систему управління ризиками підконтрольного суб'єкта, так і її частину – одну чи декілька ризикових сфер діяльності, процесів та операцій підконтрольного суб'єкта.

2.5. Керівник і члени аудиторської групи (аудитор) обирають та застосовують прийоми і процедури, які відповідають конкретним обставинам, та повинні забезпечити отримання достатніх, дійсних та необхідних доказів, які вмотивовано підкріплюють висновки.

2.6. При проведенні тестів доцільно застосовувати статистичні вибірки згідно з відповідною Настановою Департаменту.

2.7. З метою підвищення якості аудиторських послуг за результатами аудиту рекомендується провести анкетування керівництва підконтрольного суб'єкта та проаналізувати відповіді щодо якості проведеного аудиту та корисності наданих аудиторами рекомендацій (пропозицій).

¹Економічність (economy), продуктивність або ефективність (efficiency) та результативність (effectiveness) в аудиторській діяльності прийнято називати трьома “Е” – від перших літер цих термінів англійською мовою

III. ОРГАНІЗАЦІЯ ТА ПРОВЕДЕННЯ АУДИТУ

3.1. Цикл аудиту складається з таких етапів:

- підготовка до аудиту – збір інформації та планування аудиту;
- проведення аудиту (“польові роботи”) – дослідження та аналіз системи управління ризиками;
- складання звіту – підготовка проекту звіту з попередніми висновками і рекомендаціями, обговорення результатів аудиту та підписання звіту;
- моніторинг – відстеження стану та результатів впровадження рекомендацій (пропозицій).

3.2. Підготовка до аудиту є стандартною процедурою та регулюється Стандартами внутрішнього аудиту, наказами Міноборони та Департаменту.

На цьому етапі керівник аудиторської групи забезпечує отримання інформації з метою:

формування загального уявлення про: місію (мету) і цілі підконтрольного суб'єкта; ризикові сфери діяльності, процеси та операції; стан організації системи управління ризиками;

виявлення подій, що сталися в періоді, який підлягає аудиту, та мають відношення до / вплинули на управління ризиками;

складання програми аудиту.

Під час підготовки до аудиту:

збирається та аналізується інформація, яка є у розпорядженні підрозділу Служби, зокрема, матеріали попередніх внутрішніх аудитів та стан впровадження рекомендацій;

аналізується інформація, яка є у розпорядженні інших структурних підрозділів (органів) Міноборони та Генерального штабу, зокрема, інформація про результати аудитів та інших контрольних заходів, що проводилися іншими структурними підрозділами (органами) Міноборони та Генерального штабу, зовнішніми контролюючими органами (Рахунковою палатою, Держаудитслужбою тощо);

вивчається інформація з відкритих джерел інформації (зокрема, із ЗМІ, мережі Інтернет, відкритих реєстрів).

Збір інформації може здійснюватися як безпосередньо у структурних підрозділах (органах) Міноборони та Генерального штабу, інших підконтрольних суб'єктах (які володіють інформацією, що стосується підконтрольного суб'єкта, у якому планується проведення аудиту), так і шляхом направлення обов'язкових письмових запитів.

Також, по можливості, за згодою керівника підконтрольного суб'єкта, збір інформації проводиться шляхом попереднього обстеження (так званий “попередній аудит”) безпосередньо на підконтрольному суб'єкті для формування загального уявлення про:

цілі і завдання діяльності підконтрольного суб'єкта (в першу чергу тих, що визначені у стратегічних та річних планах, а також у положеннях (статутах) про підконтрольний суб'єкт);

організаційну структуру та ключових посадових осіб;

основні процеси (з урахуванням цілей та завдань кожного процесу);

матеріальну базу;

системи управління, внутрішнього контролю та управління ризиками;

інформаційні системи;

систему моніторингу та обміну інформацією.

Для забезпечення належної якості “попереднього аудиту” керівнику аудиторської групи доцільно підготувати перелік питань (опитувальні листи, анкети тощо).

За результатами аналізу одержаної інформації складається програма аудиту, проект якої перед її затвердженням рекомендується обговорити з керівництвом підконтрольного суб'єкта (це можливо зробити під час “попереднього аудиту” або організувати окрему зустріч).

В ході зустрічі керівника аудиторської групи (за потреби – за участі керівництва підрозділу Служби) з керівництвом підконтрольного суб'єкта рекомендується обговорити та уточнити:

обсяг та програму аудиторського завдання;

мету (цілі) підконтрольного суб'єкта, ризикові сфери діяльності, процеси та операції;

стан організації системи управління ризиками (чи задокументовано систему управління ризиками, чи забезпечується документальне підтвердження фактів виконання заходів контролю (“аудиторський слід”), хто відповідає за постійний моніторинг, чи здійснюються періодичні оцінки/самооцінки системи управління ризиками та виконання наданих за їх результатами рекомендацій, чи здійснюється перегляд системи управління ризиками та з якою періодичністю тощо);

проблемні питання, на які керівник підконтрольного суб'єкта пропонує звернути увагу під час аудиту.

За результатами такої зустрічі керівник аудиторської групи складає довідку, яка є робочим документом, та за необхідності вносить зміни до програми аудиту, яка затверджується в установленому порядку.

У разі неможливості проведення такої зустрічі або делегування керівником підконтрольного суб'єкта обговорення проекту програми іншим посадовим особам (крім заступника керівника підконтрольного суб'єкта) керівник аудиторської групи подає проект програми на затвердження без його обговорення.

Керівник аудиторської групи на цьому етапі відповідає за:

організацію збору інформації, в тому числі за визначення завдань кожному члену аудиторської групи щодо збору та аналізу інформації (в тому числі з відкритих джерел), підготовку і супроводження обов'язкових письмових запитів, узагальнення та аналіз одержаних даних, в тому числі

матеріалів попередніх внутрішніх аудитів, інших контрольних заходів та вжитих заходів за їх результатами;

підготовку проекту програми аудиту, організацію його обговорення з керівництвом підконтрольного суб'єкта та подання на затвердження керівнику підрозділу Служби програми аудиту,

розробку плану дій кожного члена аудиторської групи відповідно до мети аудиту та питань програми;

проведення інструктажу кожного члена аудиторської групи у безпосереднього керівника (з фахових питань), керівника аудиторської групи (з організаційних питань) та, за потреби, – у керівника підрозділу Служби.

3.3. Протягом **другого етапу** (“польові роботи”) проводиться дослідження та аналіз управління ризиками у чіткому взаємозв'язку з місією (метою) і цілями підконтрольного суб'єкта.

На початку другого етапу керівник аудиторської групи організує:

глибоке вивчення місії (мети) та цілей підконтрольного суб'єкта, викладених у стратегічних, планових, правовстановлюючих та інших документах;

аналіз наданих документів (наказів, планів, графіків, схем, журналів, доповідей, звітів, інформацій, пояснювальних записок тощо);

підготовку спеціальних опитувальних листів і проведення інтерв'ювання;

моніторинг інформації про існуючі ризики на підконтрольному суб'єкті (у т. ч. за допомогою публікацій у відкритих реєстрах та засобах масової інформації).

3.3.1. Спочатку досліджуються **організаційні питання**. Приклад форми робочого документа з дослідження організаційних питань наведено нижче.

Довідково. Робочі документи складаються в одному примірнику, зберігаються в підрозділі Служби в окремих справах та не є офіційними додатками до аудиторського звіту.

№№	Питання	Оцінка організації системи управління ризиками				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуативний	рівень 2: початковий	рівень 3: повторюваний	рівень 4: керований	
1.	Чи визначено у положенні (статуті) про підконтрольний суб'єкт завдання і функції щодо управління ризиками та відповідальність керівника за їх реалізацію?					
2.	Чи визначено у положеннях про структурні підрозділи підконтрольного суб'єкта завдання і функції щодо управління ризиками та відповідальність керівників за їх реалізацію?					

№№	Питання	Оцінка організації системи управління ризиками				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: коро- ваний	
3.	Чи визначено у посадових інструкціях (функціональних обов'язках) фахівців завдання і функції щодо управління ризиками та відповідальність за їх реалізацію?					
4.	Чи затверджено переліки функцій і процедур з їх виконання, матриці відповідальних виконавців і співвиконавців функцій та процедур, блок-схеми ходу їх реалізації, адміністративні регламенти?					
5.	Чи розроблено у 2018 році адміністративні регламенти на критичні процеси і функції та чи доведено їх до зацікавлених суб'єктів внутрішнього контролю всіх рівнів, а також підрозділів координації внутрішнього контролю в Міноборони та Генеральному штабі? <i>(п. 1.7 Інструкції № 340 – досліджується в центральних службах забезпечення)</i>					
6.	Чи створено робочу групу з визначення подій, ідентифікації та оцінки ризиків, розробки заходів контролю (далі – робоча група)?					
7.	Чи затверджено персональний склад робочої групи?					
8.	Чи вносяться зміни до складу робочої групи (наприклад, у зв'язку зі зміною назв посад, звільненням/переведенням осіб тощо)?					
9.	Чи визначено у посадових інструкціях (функціональних обов'язках) членів робочої групи відповідні завдання і функції?					

№№	Питання	Оцінка організації системи управління ризиками				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: коро- ваний	
10.	Чи затверджено порядок роботи робочої групи?					
11.	Чи проводились засідання робочої групи у поточному році (періоді аудиту)?					
12.	Чи є цьому документальні підтвердження?					
13.	Чи доведено результати роботи робочої групи до керівника?					
14.	Чи прийнято керівником управлінські рішення за результатами роботи робочої групи?					
15.	Чи затверджено у 2016 році положення про внутрішній контроль? (п. 1.7 Інструкції № 340)					
16.	Чи затверджено порядок організації та функціонування системи управління ризиками?					
17.	Чи визначено у цьому порядку:					
	категорії та види ризиків?					
	процедури, за якими здійснюється перегляд та оновлення ризиків, розподіл ризиків?					
	критерії, за якими оцінюються ризики?					
	способи реагування на ризики?					
	завдання структурних підрозділів (посадових осіб) з управління ризиками?					
	процедури, форми і терміни складання і подання інформації щодо діяльності з управління ризиками?					
	структурний підрозділ (посадових осіб), відповідальний за організацію і координацію управління ризиками в цілому за підконтрольний суб'єкт (на					

№№	Питання	Оцінка організації системи управління ризиками				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: коро- ваний	
	основі інформації інших підрозділів та посадових осіб), збір, систематизацію та аналіз інформації?					
	структурний підрозділ (посадових осіб), відповідальний за надання методологічної допомоги іншим структурним підрозділам (посадовим особам) та проведення роз'яснювальної роботи щодо управління ризиками?					
18.	Чи ознайомлено особовий склад з внутрішніми документами з управління ризиками?					
19.	Чи ознайомлюються новоприйняті фахівці з внутрішніми документами з управління ризиками?					
20.	Чи встановлено вимоги щодо навчань і підвищення кваліфікації особового складу з управління ризиками?					
21.	Чи проводяться такі навчальні заходи систематично?					
22.	Як можна охарактеризувати відсоток охоплення особового складу такими навчальними заходами?					
23.	Чи приділяє керівник та керівники структурних підрозділів належну увагу питанням управління ризиками?					
24.	Чи проводяться (проводилися) у військах (силах) у 2017 році пілотні проекти щодо функціонування системи внутрішнього контролю та управління ризиками? <i>(п. 1.7 Інструкції № 340 – досліджується лише в органах військового управління)</i>					
	Загальна оцінка					

3.3.2. Після організаційних питань досліджується процес **ідентифікації подій** у чіткому взаємозв'язку з місією (метою) і цілями підконтрольного суб'єкта.

Слід пам'ятати, що управляти абсолютно усіма ризиками неможливо. Тому для аудиту системи управління ризиками, як правило, обираються та досліджуються ризики, які безпосередньо впливають на місію (мету) та стратегічні і оперативні цілі підконтрольного суб'єкта.

У разі проведення більш масштабного аудиту досліджуються також ризики, які стосуються цілей звітування та цілей відповідності підконтрольного суб'єкта, а у разі охоплення аудитом всієї системи управління ризиками або більш детального дослідження певних видів діяльності/процесів – також ризики, що стосуються місії і цілей структурних підрозділів підконтрольного суб'єкта.

Приклад форми робочого документа з дослідження ідентифікації подій наведено нижче.

№№	Питання	Оцінка ідентифікації подій				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуативний	рівень 2: початковий	рівень 3: повторюваний	рівень 4: керований	
1.	Чи чітко сформульовано у стратегічних та планувальних документах місію (мету) та цілі підконтрольного суб'єкта?					
2.	Чи часто вони змінюються?					
3.	Чи містить положення (статут) про підконтрольний суб'єкт місію (мету) та цілі? Чи відповідають вони документам вищого рівня?					
4.	Чи відображено у внутрішніх документах підконтрольного суб'єкта його місію (мету) та цілі? Чи відповідають вони документам вищого рівня? Чи враховано зміни (якщо такі були, наприклад, у зв'язку зі зміною оргструктури)?					
5.	Чи визначено у внутрішніх документах обов'язковість наявності безпосереднього зв'язку між подіями, що ідентифікуються, та місією (метою) і цілями?					

№№	Питання	Оцінка ідентифікації подій				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: керо- ваний	
6.	Чи визначено методи ідентифікації подій та чи дотримуються вони на практиці?					
7.	Чи пов'язані безпосередньо ідентифіковані робочою групою події з місією (метою) і цілями?					
8.	Чи здійснено розмежування ідентифікованих подій на ризику та можливості?					
9.	Чи враховано можливості у діяльності підконтрольного суб'єкта?					
10.	Чи виявлено внутрішніми аудиторами (за результатами власної ідентифікації подій) інші події, не ідентифіковані робочою групою? Або – чи не ідентифіковано робочою групою “інших” (зайвих, вигаданих) подій (або подій, притаманних винятково іншим підконтрольним суб'єктам чи їх структурним підрозділам)?					
11.	Чи правильно розподілено ризику за категоріями (на зовнішні і внутрішні)?					
12.	Чи правильно розподілено ризику за видами (на нормативно-правові, операційно-технологічні, програмно-технічні, кадрові, програмно-технічні, фінансово-господарські, репутаційні, корупційні та інші)?					
13.	Чи оформлено документально та затверджено перелік ризиків?					
14.	Чи переглядається перелік ризиків:					
	систематично у визначені терміни (наприклад, шляхом самооцінки, інтерв'ювання та анкетування)?					

№№	Питання	Оцінка ідентифікації подій				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: керо- ваний	
	після настання не передбачених раніше подій?					
	за результатами внутрішніх аудитів?					
	за результатами інших контрольних заходів, проведених органами військового/господарського управління, органами забезпечення, Головною інспекцією Міноборони, ВСП ЗСУ, фінансовими органами, іншими структурами Міноборони і ЗСУ?					
	за результатами контрольних заходів Рахункової палати та Держаудитслужби?					
	за результатами контрольних заходів інших зовнішніх органів контролю?					
	у разі змін середовища (змін законодавства, пріоритетів діяльності, організаційної структури, завдань та функцій, керівництва тощо)?					
15.	Чи переглядався перелік ризиків у поточному році?					
16.	Чи завжди до переліку ризиків (своєчасно) вносилися відповідні зміни?					
	Загальна оцінка					

3.3.3. Дослідження **оцінки ризиків**, як правило, здійснюється шляхом проведення аудиторами власної оцінки ризиків (за ймовірністю їх виникнення та суттєвістю наслідків для місії (мети) і цілей, із визначенням загальної оцінки за критеріями “високий”, “середній” та “низький”) та порівняння результатів.

Приклад форми робочого документа з дослідження оцінки ризиків наведено нижче.

№№	Питання	Оцінка оцінки ризиків				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рований	рівень 4: керо- ваний	
1.	Чи володіють члени робочої групи (фахівці, які здійснюють оцінку ризиків) знаннями і досвідом у сферах, щодо яких оцінюються ризики?					
2.	Чи проводиться відповідальним підрозділом інструктаж членів робочої групи (фахівців, які здійснюють оцінку) перед проведенням оцінки?					
3.	Чи встановлені критерії для визначення ймовірності настання ризиків?					
4.	Чи співпадають ці критерії з аудиторською думкою?					
5.	Чи встановлені критерії для визначення суттєвості наслідків настання ризиків?					
6.	Чи співпадають ці критерії з аудиторською думкою?					
7.	Чи встановлені критерії для того, щоб ризики:					
	з “високою” оцінкою потребували прийняття рішень та вжиття заходів з боку керівництва та його заступників?					
	з “середньою” оцінкою потребували прийняття рішень та вжиття заходів з боку керівників нижчого рівня?					
	з “низькою” оцінкою потребували вжиття заходів з боку персоналу?					
8.	Чи переглядається оцінка ризиків:					
	систематично у визначені терміни (наприклад, шляхом самооцінки, інтерв’ювання та анкетування)?					
	після настання подій, наслідки яких відрізнялися від результатів проведеної раніше оцінки, або настання не передбачених раніше подій?					

№№	Питання	Оцінка оцінки ризиків				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рований	рівень 4: керо- ваний	
	за результатами внутрішніх аудитів?					
	за результатами інших контрольних заходів, проведених органами військового/господарського управління, органами забезпечення, Головною інспекцією Міноборони, ВСП ЗСУ, фінансовими органами, іншими структурами Міноборони і ЗСУ?					
	за результатами контрольних заходів Рахункової палати та Держаудитслужби?					
	за результатами контрольних заходів інших зовнішніх органів контролю?					
	у разі змін середовища (змін законодавства, пріоритетів діяльності, організаційної структури, завдань та функцій, керівництва тощо)?					
	Загальна оцінка					

3.3.4. Після цього вивчаються визначені **способи реагування** на ідентифіковані та оцінені ризики (зменшення, прийняття, розподіл та уникнення).

Приклад форми робочого документа з дослідження способів реагування на ризики наведено нижче.

№№	Питання	Оцінка способів реагування на ризики				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рований	рівень 4: керо- ваний	
1.	Чи щодо усіх ризиків визначено способи реагування на них?					
2.	Чи співпадають визначені способи реагування на ризики з аудиторською думкою?					

№№	Питання	Оцінка способів реагування на ризику				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рований	рівень 4: керо- ваний	
3.	Чи визначено допустимий рівень ризику?					
4.	Чи в усіх випадках прийняття ризику дотримано (не перевищено) допустимий рівень ризику?					
5.	Чи обґрунтовано уникнення ризиків? Чи не мало уникнення ризиків негативного впливу на місію (мету) та цілі?					
6.	Чи обґрунтований розподіл ризиків?					
7.	Чи немає серед ризиків, які вирішено зменшувати, таких, що потребували інших способів реагування?					
8.	Чи не створили обрані способи реагування нові “високі” ризику?					
9.	Чи не перевищують витрати обраного способу реагування на ризик вигоди від зменшення ризику чи ймовірні негативні наслідки від його настання?					
10.	Чи затверджено план заходів щодо управління ризиками (матрицю ризиків)? Чи відповідає цей документ встановленим вимогам? <i>В органах військового управління також досліджується, чи забезпечується функціонування централізованої системи планування та управління ризиками у ЗСУ, в рамках якої розробляються та затверджуються плани управління ризиками на 2017 рік Збройних Сил України, командувань видів,</i>					

№№	Питання	Оцінка способів реагування на ризику				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: керо- ваний	
	<i>Високомобільних десантних військ, Сил спеціальних операцій, органів військового управління,, центральних служб забезпечення? (п. 1.7 Інструкції № 340).</i>					
11.	Чи здійснюється систематичний його перегляд і затвердження?					
12.	Чи застосовано в управлінні ризиками модель “трьох ліній оборони”?					
13.	Чи визначено підрозділи (посадових осіб), які належать до “першої”, “другої” та “третьої” ліній оборони?					
	Загальна оцінка					

3.3.5. Досліджуючи **заходи контролю**, слід проаналізувати не лише затверджені заходи, а й фактичне їх виконання (шляхом проведення тестів).

Приклад форми робочого документа з дослідження заходів контролю наведено нижче.

№№	Питання	Оцінка заходів контролю				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: керо- ваний	
1.	Чи до кожного ризику визначено заходи контролю?					
2.	Який вид заходів контролю застосовується найчастіше:					
	превентивні?					
	директивні?					
	виявляючі?					
	коригуючі?					
3.	Чи дотримується розумний баланс у застосуванні превентивних, директивних, виявляючих та коригуючих заходів контролю?					
4.	Чи співпадають визначені заходи контролю з аудиторською думкою?					

№№	Питання	Оцінка заходів контролю				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: коро- ваний	
5.	Чи достатніми, на думку аудитора, є визначені заходи (чи забезпечать вони, у разі неухильного застосування, достатній рівень впевненості з урахуванням визначеного допустимого рівня ризиків)?					
6.	Чи виявлено ризики, щодо яких не встановлено відповідні (достатні) заходи контролю?					
7.	Чи дотримано розумний баланс між вартістю запроваджених заходів контролю та вигодами від їх запровадження?					
8.	Чи визначені виконавці та терміни виконання заходів контролю?					
9.	Чи внесено зміни щодо виконавців у разі ротації персоналу (звільнення, переміщення, навчання заочною формою, декретна відпустка тощо)?					
10.	Чи доведено до персоналу вимоги щодо здійснення заходів контролю?					
11.	Чи застосовуються на практиці затверджені заходи контролю у повному обсязі?					
12.	Чи не виявлено випадків “виключень” щодо (незастосування в окремих випадках) заходів контролю (наприклад, у зв’язку з терміновістю, у передвихідні та передсвяткові дні, перед відпустками, звільненням тощо)?					
13.	Чи встановлено вимоги щодо обов’язковості належного документального підтвердження (“аудиторський слід”) факту того, що захід контролю було					

№№	Питання	Оцінка заходів контролю				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: коро- ваний	
	здійснено (наприклад, шляхом візування, погодження, проставлення штампу, складання доповідної записки, іншого документа)?					
14.	Чи усі заходи контролю, щодо яких проведено тестування, містять “аудиторський слід”?					
15.	Чи виявлено випадки, коли заходи контролю “не спрацювали” (не попередили чи не обмежили ризик або не зменшили негативні наслідки від його настання)?					
16.	Яка питома вага кількості та наслідків таких заходів контролю?					
17.	Чи встановлено вимоги щодо необхідності чіткого розмежування обов’язків і повноважень з внутрішнього контролю в частині, що стосується заходів контролю?					
18.	Чи встановлено випадки нерозмежування обов’язків і повноважень з внутрішнього контролю в частині, що стосується заходів контролю?					
19.	Наскільки поширеною є така практика?					
20.	Чи переглядаються заходи контролю:					
	систематично у визначені терміни (наприклад, шляхом самооцінки, інтерв’ювання та анкетування)?					
	після настання подій, наслідки яких відрізнялися від результатів проведеної раніше оцінки, або настання не передбачених раніше подій?					
	за результатами внутрішніх аудитів?					

№№	Питання	Оцінка заходів контролю				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: коро- ваний	
	за результатами інших контрольних заходів, проведених органами військового / господарського управління, органами забезпечення, Головною інспекцією Міноборони, ВСП ЗСУ, фінансовими органами, іншими структурами Міноборони і ЗСУ?					
	за результатами контрольних заходів Рахункової палати та Держаудитслужби?					
	за результатами контрольних заходів інших зовнішніх органів контролю?					
	у разі змін середовища (змін законодавства, пріоритетів діяльності, організаційної структури, завдань та функцій, керівництва тощо)?					
	Загальна оцінка					

3.3.6. Дослідження **інформації і комунікації** проводиться в частині, що стосується системи управління ризиками.

Приклад форми робочого документа з дослідження інформації і комунікації наведено нижче.

№№	Питання	Оцінка інформації і комунікації				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: коро- ваний	
1.	Чи встановлено правила (регламенти, процедури) інформування керівництва про ризики (знизу вверху)?					
2.	Чи дотримуються вони на практиці?					
3.	Якщо так, чи приймаються керівництвом рішення щодо реагування на ризики та чи запроваджуються заходи контролю?					

№№	Питання	Оцінка інформації і комунікації				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: коро- ваний	
4.	Чи інформується керівництво про випадки, коли запроваджені заходи контролю не застосовуються на практиці?					
5.	Чи інформується керівництво про випадки, коли заходи контролю не досягають мети (не спрацювали)?					
6.	Чи доводиться до керівників нижчого рівня та персоналу інформація щодо ризиків та запроваджені заходи контролю (зверху вниз)?					
7.	Чи обговорюються на нарадах, інших заходах питання системи управління ризиками?					
8.	Якщо так, то чи приймаються письмові рішення?					
9.	Чи використовуються неформальні канали доведення і обміну інформацією?					
10.	Чи достатньо інформації для прийняття обґрунтованих управлінських рішень?					
11.	Чи використовуються зовнішні джерела інформації в системі управління ризиками?					
12.	Чи до всіх зацікавлених осіб доводиться інформація про:					
	результати самооцінки, інтерв'ювання та анкетування щодо системи управління ризиками?					
	настання не передбачених раніше подій?					
	результати внутрішніх аудитів?					
	результати інших контрольних заходів, проведених органами військового/господарського управління, органами забезпечення, Головною інспекцією Міноборони, ВСП ЗСУ, фінансовими органами, іншими структурами Міноборони і ЗСУ?					
	результати контрольних заходів Держаудитслужби?					

№№	Питання	Оцінка інформації і комунікації				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: коро- ваний	
	результати контрольних заходів інших зовнішніх органів контролю?					
	зміни середовища (зміни законодавства, пріоритетів діяльності, організаційної структури, завдань та функцій, керівництва тощо)?					
13.	Чи здійснюється інформаційний обмін між суб'єктами внутрішнього контролю на різних рівнях управління та центральними службами забезпечення з питань планування заходів з управління ризиками та розробки адміністративних регламентів? <i>(п. 1.7 Інструкції № 340)</i>					
14.	Чи забезпечено доступ до інформаційних ресурсів, використання яких є необхідним для системи управління ризиками?					
15.	Як можна охарактеризувати ступінь доступу у порівнянні з необхідним?					
16.	Чи використовується в системі управління ризиками відповідне програмне забезпечення?					
17.	Як можна охарактеризувати ступінь використання програмного забезпечення у порівнянні з необхідним?					
18.	Чи впроваджено (враховано) у 2019 році затверджені регламенти і процеси у програмне забезпечення автоматизованих систем обліку та руху матеріально-технічних засобів Збройних Сил України, автоматизованої системи кадрового менеджменту та інших (за пріоритетністю)? <i>(п. 1.7 Інструкції № 340)</i>					

№№	Питання	Оцінка інформації і комунікації				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рюваний	рівень 4: коро- ваний	
19.	Чи складаються та подаються до органів військового управління за підпорядкованістю у визначені ними терміни: плани заходів щодо управління ризиками (дод. 2 до Інструкції № 340); інформація з ідентифікації та оцінки ризиків (дод. 4 до Інструкції № 340); річні звіти про забезпечення гарантій згідно звизначеними підрозділом координації Міноборони формою, порядком та термінами?					
20.	Чи надано до 31 жовтня у дослідженому періоді органами військового управління, частинами та установами безпосереднього підпорядкування Генерального штабу до Відділу внутрішнього контролю Генштабу узагальнену інформацію з ідентифікації та оцінки ризиків, згруповану за напрямками діяльності центральних служб забезпечення і пропозиції до Плану заходів щодо управління ризиками у Збройних Силах України? (п. 5.4 Інструкції № 340)					
	Загальна оцінка					

3.3.7. При дослідженні **моніторингу** вивчаються як встановлені регламенти щодо його проведення, так і фактичні результати моніторингу в частині, що стосується системи управління ризиками.

Приклад форми робочого документа з дослідження моніторингу наведено нижче.

№№	Питання	Оцінка моніторингу				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуа- тивний	рівень 2: почат- ковий	рівень 3: повто- рований	рівень 4: керо- ваний	
1.	Чи встановлено обов'язковість проведення постійного моніторингу?					
2.	Чи визначено відповідальних осіб та порядок його проведення?					
3.	Чи дотримуються ці вимоги на практиці?					
4.	Якщо так, то чи є цьому документальне підтвердження ("аудиторський слід")?					
5.	Чи приймаються рішення за результатами постійного моніторингу?					
6.	Чи встановлено обов'язковість проведення періодичних оцінок системи управління ризиками?					
7.	Чи визначено відповідальні структурні підрозділи та порядок їх проведення?					
8.	Чи дотримуються ці вимоги на практиці?					
9.	Якщо так, то чи є цьому документальне підтвердження?					
10.	Чи приймаються рішення за результатами періодичних оцінок?					
11.	Чи рішення, прийняті за результатами постійного моніторингу та періодичних оцінок, переважно спрямовані на:					
	виправлення вже допущених помилок, недоліків і порушень?					
	покарання винних осіб?					
	постійне удосконалення системи управління ризиками?					
12.	Чи виконуються прийняті рішення?					
13.	Як можна охарактеризувати повноту виконання прийнятих рішень?					

№№	Питання	Оцінка моніторингу				Обґрунтування оцінки (посилання на докази)
		рівень 1: ситуативний	рівень 2: початковий	рівень 3: повторюваний	рівень 4: керований	
14.	Наскільки виконання прийнятих рішень позитивно впливає на стійкість системи управління ризиками та її удосконалення?					
	Загальна оцінка					

3.3.8. Аудит ефективності (performance audit) управління ризиками може досліджувати питання економічності/економності (economy), продуктивності/ефективності (efficiency) та результативності (effectiveness) (див. пункт 2.4 цієї Тимчасової настанови).

При оцінці економічності/економності аудит зосереджується на питаннях мінімізації затрат/внеску (в цілому на систему управління ризиками, на отриманий продукт або на одиницю продукту). Питаннями аудиту можуть бути: чи не витрачаються зайві ресурси на управління ризиками? чи існують шляхи зменшення обсягу ресурсів, що витрачається на управління ризиками у певній сфері/виді діяльності/процесі? чи немає зайвих або “дорогих” заходів контролю, від яких можна відмовитися або які можна замінити дешевшими? чи можна забезпечити одержання певної інформації за менший обсяг ресурсів? чи можна зменшити вартість звітів про результати самооцінки?

При оцінці продуктивності/ефективності аудит зосереджується на співвідношенні між вартістю продукту та ресурсами, витраченими на його створення. Наголос може робитися як на продуктивності (отриманні максимального обсягу продукту за попередньо визначений/виділений обсяг ресурсів), так і на ефективності (отриманні максимального обсягу продукту за мінімальний обсяг ресурсів). Питаннями можуть бути: чи існують шляхи підвищення ефективності системи управління ризиками? чи можна одержати ту саму або більшу кількість продукту (наприклад, заходів контролю, одержаної інформації, звітів про результати самооцінки) за менший обсяг ресурсів? чи можна одержати більший обсяг продукту за той самий обсяг ресурсів?

При оцінці результативності аудит зосереджується на результатах – ступені відповідності результатів управління ризиками визначеним меті (місії) та цілям. Результативність може оцінюватися як з урахуванням визначеного обсягу ресурсів, так і без його врахування. Наприклад, для оцінки ступеня відповідності фактичних результатів із визначеними операційними цілями доцільно використовувати інформацію, наведену у графах 5 “Очікувані результати від впровадження заходів контролю (операційна ціль N)” та 6 “Заходи моніторингу (стан впровадження з зазначенням конкретних

результатів)» Плану заходів щодо управління ризиками (додаток 2 до Інструкції № 340). Для оцінки ступеня досягнення стратегічних цілей доцільно використовувати ключові показники ефективності (КПІ) тощо. Прикладами показників результативності можуть бути: вигоди від удосконалення процесів; збільшення обсягу надходжень або економія ресурсів; попередження втрат або неефективного використання ресурсів; зменшення кількості, обсягу або питомої ваги помилок, виявлених заходами подальшого контролю; запобігання іміджевим втратам тощо.

При проведенні аудиту ефективності системи управління ризиками можуть використовуватися положення Настанови з проведення аудиту ефективності виконання бюджетних програм (підпрограм), затвердженої наказом Департаменту від 21.10.2012 № 4.

3.3.9. Під час проведення аудиту кожного елемента системи управління ризиками доцільно здійснювати збір та оцінку даних щодо того:

наскільки процеси управління ризиками допомагають у реалізації загальної стратегії Міноборони (ЗСУ) та досягненню місії (мети) і цілей підконтрольного суб'єкта;

наскільки існуюча система управління ризиками забезпечує економне, ефективне та результативне управління ресурсами підконтрольним суб'єктом.

IV. СКЛАДАННЯ ЗВІТУ

4.1. Порядок складання, обговорення та підписання аудиторського звіту регулюється Стандартами внутрішнього аудиту, наказами Міноборони та Департаменту.

4.2. При формуванні аудиторського висновку враховуються результати роботи, проведеної аудиторами під час попередніх етапів, та надається загальна оцінка системи управління ризиками за такими рівнями зрілості²:

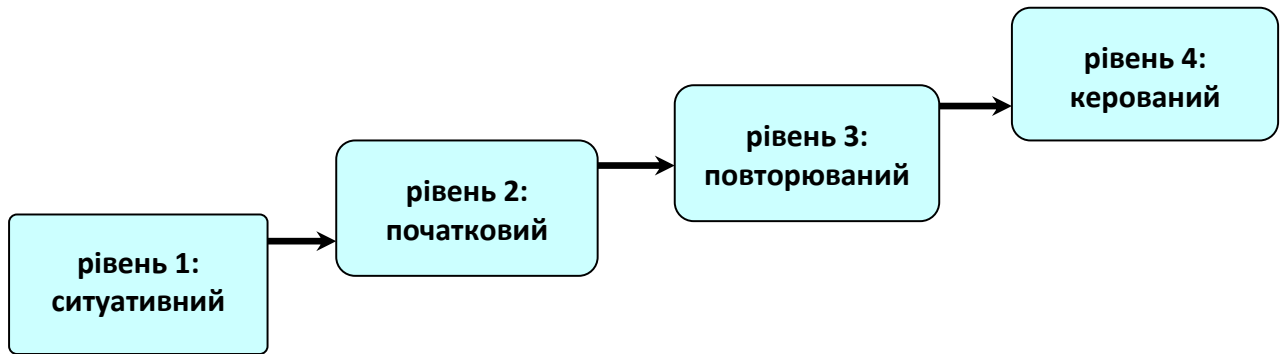
ситуативний рівень – управління ризиками здійснюється “ситуативно”, що відповідає негативному висновку;

початковий рівень – управління ризиками здійснюється у невеликих масштабах (експерименти, “пілотні проекти” тощо), що відповідає слабо-позитивному висновку;

повторюваний рівень – управління ризиками широко використовується та є формалізованим, що відповідає задовільно-позитивному висновку;

керований рівень – управління ризиками лежить в основі культури підконтрольного суб'єкта та у постановці стратегії, що відповідає безумовно-позитивному висновку.

² 3. Практичні вказівки щодо впровадження фінансового управління і контролю та посилення управлінської підзвітності (відповідальності) в органах державної влади України [Електронний ресурс]. – Режим доступу: <https://minfin.gov.ua/news/view/metodychni-posibnyky-shchodo-dfvk?category=borg&subcategory=derzhavnyi-vnutrishnii-finansovyi-kontrol>



4.3. Основні характеристики рівнів зрілості підконтрольного суб'єкта (або його структурного підрозділу) нижче наведено у таблиці.

Рівні зрілості системи управління ризиками та їх характеристики

	Рівень 1: Ситуативний	Рівень 2: Початковий	Рівень 3: Повторюваний	Рівень 4: керований
Визначення	Керівництво не усвідомлює своєї потреби знати про ризики. Системний підхід до роботи з ризиками відсутній. Керівництво реагує на події, що вже сталися. Відсутні спроби або незначна кількість спроб вчитися на минулому або готуватись до майбутніх подій і проектів.	Розпочато / проводяться експерименти з управління ризиками (наприклад, "пілотні проекти" або поетапне запровадження) із залученням невеликої кількості осіб. Системний підхід до роботи з недоліками та ризиками відсутній. Керівники усвідомлюють потенційні переваги від управління ризиками, однак на практиці застосовують його неефективно (відсутня цілісна система управління ризиками).	Управління ризиками вбудовано майже в усі процеси підконтрольного суб'єкта та застосовується майже до усіх видів діяльності (проектів). Запроваджено формалізовані універсальні (загальні) процеси управління ризиками. Переваги від управління ризиками зрозумілі на усіх рівнях підконтрольного суб'єкта, хоча й не завжди послідовно досягаються.	В усіх сферах діяльності підконтрольного суб'єкта існує свідомо культура та застосовуються проактивні підходи до управління ризиками. Інформація про ризики активно використовується для вдосконалення діяльності та досягнення мети і цілей підконтрольного суб'єкта в економічний, ефективний та результативний спосіб.
Культура	Керівництво не усвідомлює ризики та не втручається в управління ними. Поширеними є спротив та небажання змін. Існує стійка	Процеси управління ризиками можуть розглядатись як додатковий елемент із змінними перевагами. Вище керівництво	Затверджено політику (стандарти, наказ, настанова, методичні рекомендації, положення тощо) щодо управління ризиками.	Вище керівництво є прикладом відданості управлінню ризиками, використовує інформацію про ризики для

	Рівень 1: Ситуативний	Рівень 2: Початковий	Рівень 3: Повторюваний	Рівень 4: керований
	тенденція до продовження роботи у незмінному режимі, навіть попри її неефективність. Винним є той, хто приносить “погані новини” (наприклад, аудитор або бухгалтер).	заохочує, але не вимагає використання управління ризиками. Управління ризиками використовується лише для певних видів діяльності (проектів).	Переваги визнані та прийняті. Вище керівництво вимагає звітування щодо управління ризиками. На управління ризиками виділено ресурси (зокрема, людські). Інформація про “погані новини” стосовно ризиків приймається (сприймається адекватно).	прийняття рішень, заохочує та винагороджує за проактивне управління ризиками. Філософією підконтрольного суб’єкта приймається (сприймається адекватно) те, що люди роблять помилки.
Процеси	Формалізовані процеси (наприклад, блок-схеми, адміністративні регламенти тощо), план управління ризиками тощо відсутні. Спроби застосувати принципи управління ризиками відсутні або їх кількість є незначною, причому такі спроби здійснюються лише на вимогу (наприклад, за результатами аудиту).	Універсальні формалізовані процеси відсутні, навіть при тому, що застосовуються окремі формалізовані заходи контролю. Ефективність процесу значною мірою залежить від навиків команди управління ризиками, яка працює у певному виді діяльності (над проектом), а також від наявності зовнішньої підтримки. Весь персонал по роботі з ризиками закріплений за видом діяльності (проектом).	Універсальні формалізовані процеси застосовуються майже до усіх видів діяльності (проектів) та об’єднано в єдину систему. Здійснюється активне управління бюджетом, призначеним для управління ризиками на усіх рівнях. Потреба у зовнішніх ресурсах і підтримці є обмеженою. Затверджено матрицю ризиків. Ключові постачальники беруть участь у процесі управління ризиками. Передача інформації керівництву підконтрольного суб’єкта може здійснюватися неформально.	Все процеси підконтрольного суб’єкта враховують управління ризиками (базуються на ризиках). Культура управління ризиками домінує в підконтрольному суб’єкті. Процеси регулярно оцінюються та покращуються. План управління ризиками (матриця ризиків) використовується у щоденному режимі з отриманням послідовної інформації стосовно вдосконалення діяльності. Ключові постачальники та клієнти беруть участь у процесі управління ризиками. Використовується прямий канал передачі

	Рівень 1: Ситуативний	Рівень 2: Початковий	Рівень 3: Повторюваний	Рівень 4: керований
				інформації керівництву підконтрольного суб'єкта.
Досвід	Розуміння принципів управління ризиками та термінології, розуміння або досвід роботи із заходами контролю відсутні.	Лише незначна кількість персоналу пройшла навчання (або жодних тренінгів не проводилося).	Наявні власний досвід та персонал, який пройшов навчання і володіє навиками управління ризиками. Розроблено та використовуються певні процедури та заходи контролю.	Весь персонал усвідомлює ризики та спроможний використовувати основні навички управління ризиками. Навчання та обмін досвідом розглядається як частина процесу. Проводяться регулярні тренінги для того, щоб персонал досяг вищого рівня знань, досвіду та навиків.
Застосування	Системне застосування відсутнє. Ресурси на управління ризиками не виділяються. Інструменти управління ризиками не використовуються. Ідентифікація і оцінка ризиків не проводиться.	Ресурси на управління ризиками виділяються та використовуються непослідовно. Використовується лише методологія ідентифікації та оцінки ризиків.	Управління ризиками застосовується майже до всіх видів діяльності (проектів) на щоденній основі, на що виділяються ресурси. Застосовується комплексний набір інструментів та заходів контролю. Використовується методологія кількісної та якісної оцінки ризиків.	Управління ризиками застосовується до всіх видів діяльності (проектів) на постійній основі, на що виділяються ресурси. Рішення приймаються та звітування здійснюється на підставі оцінки ризиків. Застосовуються новітні інструменти, заходи контролю та методологія якісної і кількісної оцінки ризиків. Головний акцент робиться на використанні дійсних та надійних історичних баз даних.

4.4. Для кращого інформування про важливість результатів аудиту та терміновість впровадження рекомендацій (виконання пропозицій) вони розподіляються за ступенями:

критичні – стосуються найважливіших проблем або недоліків в колективі, системі, діяльності або процесі, що може відчутно вплинути на досягнення місії (мети) і цілей, діяльність або репутацію підконтрольного суб'єкта та потрапить у річний звіт директора Служби;

важливі – стосуються важливих проблем або недоліків в колективі, системі, діяльності або процесі, що, втім, не матиме відчутного впливу на досягнення місії (мети) і цілей, діяльність або репутацію підконтрольного суб'єкта;

бажані – стосуються проблем або недоліків, усунення яких покращить управління ризиками або управління фінансовими, матеріальними чи іншими ресурсами, але без цього місію (мету) і цілі і так вдасться досягати, хоча і з нижчою ефективністю.

4.5. Проект аудиторського звіту в установлені строки передається для ознайомлення керівництву підконтрольного суб'єкта та визначається час для обговорення проекту звіту.

У разі надання керівництвом підконтрольного суб'єкта під час обговорення проекту звіту обґрунтованих коментарів чи зауважень (із додаванням завірених копій документів, інших доказів) керівник аудиторської групи (аудитор) оцінює їх та у разі прийняття аргументів може врахувати їх в остаточній редакції аудиторського звіту.

4.6. Аудиторський звіт підписується у встановленому порядку.

4.7. У разі наявності неврахованих коментарів (зауважень) їх розгляд здійснюється в установленому порядку.

4.8. Копії аудиторського звіту (резюме або витяг зі звіту) за рішенням керівництва Департаменту можуть направлятися зацікавленим структурним підрозділам Міноборони, Генерального штабу, іншим органам.

4.9. У разі надання безумовно-позитивного висновку (рівень 4: керований) або висновку щодо ефективності системи управління ризиками підконтрольного суб'єкта, за рішенням керівника Служби, ініціюється поширення результатів такого аудиту серед інших підконтрольних суб'єктів як позитивний досвід.

V. МОНІТОРИНГ

5.1. Підрозділи Служби здійснюють моніторинг і облік результатів впровадження рекомендацій (пропозицій) в установленому порядку.

