

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО ФИЗИОЛОГИЯ НА РАСТЕНИЯТА И ГЕНЕТИКА

УТВЪРДИЛ
ДИРЕКТОР:
(проф. д-р Валя Василева)

СТРАТЕГИЯ ЗА УПРАВЛЕНИЕ НА РИСКА
В ИНСТИТУТА ПО ФИЗИОЛОГИЯ НА РАСТЕНИЯТА И ГЕНЕТИКА
КЪМ БЪЛГАРСКАТА АКАДЕМИЯ НА НАУКИТЕ
2023-2025

януари 2023 г.

I. ОБЩИ ПОЛОЖЕНИЯ

Настоящата Стратегия за управление на риска в Института по физиология на растенията и генетика (ИФРГ) към Българската академия на науките (БАН) е изготвена в изпълнение на изискванията на Закона за финансовото управление и контрол в публичния сектор (ЗФУКПС).

Целта на Стратегията за управление на риска е да опише етапите, през които преминава процесът по управление на риска, използвания подход, отговорните лица (звена/структури) и основните изисквания към процеса. Стратегията ще подпомогне ръководството на ИФРГ, ръководителите на лабораториите и служителите в ИФРГ при осъществяване на функциите им, свързани с:

- идентифициране и оценка на рисковете, застрашаващи постигането на целите;
- определяне на подходящи действия в отговор на рисковете;
- документиране на резултатите от управлението на риска на всеки етап.

Стратегията въвежда унифициран и стандартизиран подход за управление на риска във всички звена на ИФРГ, който позволява навременно предприемане на адекватни действия спрямо идентифицираните рискове, застрашаващи постигането на целите на всяка конкретна структурна единица. Унифициран и стандартизиран подход означава:

- **Единна теоретична база и терминология:** общоприета дефиниция за риск, единна система за идентифициране, оценка и контрол на рисковете и основни етапи (стъпки) на процеса по управление на риска;
- **Общо-приложима методология за идентифициране и оценка на рисковете:** методологията се прилага във всички структурни единици от всички служители в ИФРГ;
- **Разбиране за възможните реакции в отговор на риска:** ограничаване, прехвърляне, толериране и прекратяване на риска, вземане на решение относно подходящата реакция и предприемането на конкретни действия в подкрепа на това решение;
- **Определяне на състава, ролята и отговорностите на Комитета по риска;**
- **Приемственост и устойчивост на дейностите:** управлението на риска в ИФРГ е непрекъснат процес, отнасящ се до всички структури, дейности и нива в организацията. Адекватното управление на риска изисква редовна комуникация, мониторинг и докладване на резултатите от процеса по управление на риска.

Целите на Стратегията за управление на риска в ИФРГ са свързани с:

- Изграждане на съзнание и разбиране за процеса по управление на риска на всички нива в ИФРГ;
- Изграждане на организационна култура по отношение на управлението на риска и на отговорност, свързана с управлението на риска на всички нива в Института;
- Обхващане на всички рискове и на тяхното добро управление в рамките на риск-апетита;
- Внедряване на управлението на риска като част от процеса по вземане на решения. Това включва свързване на идентифицираните рискове и контролни дейности със стратегическите и оперативни цели на академията, като част от процеса по годишно планиране;
- Постигане на съответствие с изискванията на чл. 8 от Закона за финансовото управление и контрол в публичния сектор (ЗФУКПС) за Годишно докладване за функционирането, адекватността, ефикасността и ефективността на системите за финансово управление и контрол¹ (СФУК/ВК/СВК).

Стратегията за управление на риска се утвърждава от директора на ИФРГ, след съгласуване с Комитета по риска в ИФРГ. Стратегията за управление на риска следва да се актуализира на всеки три години и/или при настъпване на съществени промени в рисковата среда.

I. ОБЩ ПРЕГЛЕД НА ПРОЦЕСА ПО УПРАВЛЕНИЕ НА РИСКА В ИФРГ

1. Дефиниции

1.1. Управление на риска

Дефиницията за управлението на риска се съдържа в чл. 12, ал. 2 на Закона за финансовото управление и контрол в публичния сектор: *„Управлението на риска включва идентифициране, оценяване и контролиране на потенциални събития или ситуации, които могат да повлияят негативно върху постигане целите на организацията, и е предназначено да даде разумна увереност, че целите ще бъдат постигнати“.*

Управлението на риска в ИФРГ е динамичен процес, обвързан с непрекъснато променящата се среда, в която Институтът функционира. Различните фази на процеса се осъществяват непрекъснато във времето и отразяват настъпващите промени. В тази връзка, актуализацията на целите, вероятността от настъпване на риск и възможното влияние, мерките, които се определят за реакция на рисковете, са също динамични и трябва да се наблюдават и актуализират непрекъснато. Процесът по управление на риска трябва да се изпълнява като комбинация от периодични (поне веднъж в годината) и текущи (при промяна на риск средата или друга необходимост) мерки и дейности. Процесът по управление на риска е отговорност на Директора на ИФРГ, но конкретни функции и отговорности по неговото изпълнение съществуват на всички йерархични нива във всички структурни единици на Института. От изключителна важност за ефективността на процеса е ангажираността и разбирането на ръководството и служителите в ИФРГ.

1.2. Риск

Рискът е събитие, което ще повлияе върху постигане на целите на Института. Рискът се измерва с неговия ефект и с вероятността от настъпването му. Тази дефиниция за риск се съдържа в §1, т. 5 от допълнителните разпоредби на Закона за финансово управление и контрол в публичния сектор.

1.3. Разумна увереност

Представява задоволително ниво на увереност, което изисква разходите за вътрешен контрол да не надхвърлят очакваните ползи от него. Концепцията за разумна увереност е признание, че не е възможно да се твърди абсолютно и със сигурност, че дадено неблагоприятно събитие няма да се случи въпреки взетите мерки и предприетите действия. Никой не може да постигне абсолютна (100%) увереност поради многобройни фактори, произтичащи от ограничените финансови и други ресурси, ограниченията на източниците на информация, човешките грешки и т.н.

1.4. Идентифициране на риска

Идентифициране на вътрешни и външни събития, които могат да застрашат постигането на целите на Института.

1.5. Оценка на риска

Това е процес, състоящ се от определяне на степен на вероятност от сбъдването на идентифицирания риск и определяне на степен на влияние (ефект) върху целите на организацията при неговото настъпване.

1.6. Вероятност

Представява възможността дадено събитие да се случи или с други думи колко е вероятно дадено събитие да се прояви.

1.7. Влияние (ефект)

Представява описание и оценка на това какви биха могли да бъдат последствията/въздействието от настъпило събитие. Ефектът може да бъде както отрицателен, така и положителен.

1.8. Присъщ риск

Това е рискът, свързан с естеството на дейността на организацията при липса на каквито и да е действия (контроли) за смекчаване на вероятността или на ефекта от неговото проявление.

1.9. Остатъчен риск

Това е нивото на влияние и вероятност от риск, което остава след реакцията (контрола) на Ръководството към риска. След предприемане на конкретни действия (реакция на риска) продължава да съществува риск, който се нарича **остатъчен риск**, и по същество изразява факта, че рискът не може да бъде премахнат изцяло. Отговорност на Директора е да реши дали равнището на остатъчния риск е приемливо за Организацията или е необходимо да бъдат предприети допълнителни действия за неговото намаляване.

1.10. Реакция на риска

Представяват мерки/действия за приемане, ограничаване, прехвърляне или прекратяване на риска.

1.11. Риск-апетит

Това е нивото на риск, което организацията е склонна да приеме при изпълнение на своята мисия, без да бъде застрашено постигането на целите. Комитетът по риска, с одобрението на Директора, определя риск-апетита на ИФРГ. Ръководителите на лабораториите са отговорни за определянето на риск-апетита на звената, които ръководят.

Нивото на риск-апетита, определено от Комитета по риска и одобрено от Директора, и от ръководителите на лаборатории, има директно отношение към реакцията спрямо даден риск, т.е. първо дали Институтът ще ограничи, прехвърли, толерира или прекрати риска, и второ, как и чрез какви дейности ще бъде изразена тази реакция. Реакцията на риска е в пряка връзка с риск рейтинга.

2. Роли и отговорности

Директорът трябва да създаде условия за формулиране на ясни, конкретни и измерими цели, осигурени с конкретни по размер и източник ресурси, в съответствие със съществуващите нормативни изисквания и добри практики. Той отговаря за създаването и поддържането на култура на управление на риска в звеното. Предвид факта, че Директорът определя „тона на върха“ в звеното, той трябва да демонстрира с поведението си разбиране на важността и подкрепа за дейностите по управление на риска. Директорът отговаря за определяне на мисията, визията и стратегическите цели на Организацията. Предвид значението на правилното целеполагане за ефективността на системите за вътрешен контрол и в частност на управлението на риска, тези отговорности на Директора са ключови за реалното функциониране на управлението на риска като процес.

2.1. Директор на институт от системата на БАН

Идентифицирането, оценката и управлението на рисковете, застрашаващи постигането на целите на ИФРГ, е част от управленската отговорност, дефинирана в чл. 7, ал. 1 от ЗФУКПС на директорите на академичните институти и други самостоятелни структурни звена в системата на БАН. При реализиране на този аспект от управленската си отговорност, Директорът се подпомага от Комитет по риска в ИФРГ. Функциите и правомощията на Комитета по риска, неговите членове и председател, съгласно тази Стратегия, се определят със заповед от Директора, който следи за нейното изпълнение.

Комитет по риска се сформира на основание чл. 4, ал. 1, чл. 7, ал. 1 и 2, чл. 12, ал. 1, 3 и 4 от Закона за финансовото управление и контрол в публичния сектор, с цел гарантиране на постоянно наблюдение на процесите по управление на рисковете в ИФРГ.

Директорът следва да определи лица, отговорни за управлението на риска (отговорници по риска), които следва да имат водеща роля в процеса по управление на риска в Института и организират попълването на риск-регистрите в съответните организации.

2.2. Комитет по риска/Риск-мениджмънт

Комитетът по риска в ИФРГ е работна група, чиято основна роля е централизираното управление на риска в Института. Комитетът по риска трябва да се състои от минимум пет члена, които са специалисти в различни области, свързани с функциите на Института. Членовете на Комитета следва да притежават добро разбиране за дейностите на ИФРГ, както и експертни познания, умения и опит за оценяване и управление на комплексни рискови фактори. Добра практика е в Комитета да участват лица на ръководни длъжности, в съответствие с управленската отговорност, която носят при изпълнение на техните задължения. Комитетът по риска се ръководи от Председател, който изпълнява функцията на Риск-ръководител, който е на достатъчно високо ниво в Организацията и познава добре структурата и дейността, нейните стратегически и годишни цели, както и има достатъчно познания за същността на процеса по управление на риска.

Предвидено е Риск-ръководителят в средносрочен план да придобие подходящи сертификати за управление на риска.

Функциите и правомощията на Комитета по риска, съгласно тази Стратегия, са свързани с това да:

- Координира, организира и информационно обезпечава дейностите по идентифициране и оценка на риска и определя на реакции на риска;
- Осигурява отразяването на рисковете и тяхната оценка, на резултатите от извършените по управление на риска действия, сроковете, в които действията ще бъдат предприети и отговорните лица, в специален документ - риск-регистър, както и подsigурява неговото периодично/редовно актуализиране;
- Подпомага ръководството на ИФРГ при определянето на риск-апетита и даване на указания относно приемливите нива на риск;
- Изпълнява методологически функции по управление на риска - подпомага и консултира „собствениците на риска“ при прилагането на методите и техниките на идентифициране и оценка на риска и при определяне на реакциите на риска;
- Консултира и организира провеждането на обучения по теми, свързани с управлението на риска;
- Организира и координира обмяната на знания и информация по отношение на управлението на риска между трите линии на защита;
- Организира осъществяването на мониторинг на управлението на риска, с цел да се установи дали след прилагането на избраната реакция, рискът е бил намален до приемливо за организацията равнище и ако е необходимо, да се изберат подходящи допълнителни действия. В резултат от мониторинга, управлението на риска се наблюдава непрекъснато на всеки един етап като част от общия процес на управление, заедно с текущите промени, които могат да повлияят на целите или на възможността те да бъдат постигнати, за да придобие увереност, че процесът по управление на риска е ефективен и ефикасен;
- Докладва на Директора обобщена информация по отношение управлението на риска под формата на отчети. При необходимост от предприемане на коригиращи действия в резултат от мониторинга, Риск-мениджмънтът докладва на Директора и организира и координира тяхното разработване в съответствие със Стратегията за управление на риска.

2.3. Ръководители на лаборатории (Риск-собственици)

Ръководителите на лаборатории формират първата линия на защита. В тази връзка те са пряко отговорни за управлението на рисковете, както и за прилагането на коригиращи действия при наличие на недостатъци в процесите и контрола. Те отговарят за определянето на цели в звената, които ръководят, като разработват и прилагат оперативни/годишни планове. Ръководителите носят отговорност за идентифицирането, оценката и управлението на рисковете, застрашаващи постигането на целите на звената.

Отговорностите им по отношение на управлението на риска включват следното:

- Всеки ръководител на лаборатория е „собственик на риска“ по отношение на целите, функциите и дейностите, стоящи за изпълнение пред ръководеното от него звено;
- Като собственици на риска ръководителите на лабораториите идентифицират и оценяват рисковете съобразно подхода, утвърден със Стратегията за управление на риска в ИФРГ. Отговорността на всеки риск-собственик е преди всичко по отношение на идентифицирането и оценката на рискове, които стоят пред ръководеното от него звено/дейност, и на второ място по отношение на идентифицирането и оценката на рисковете, стоящи пред организацията като цяло;
- Ръководителите на лаборатории са отговорни за анализ и актуализация на контролните дейности, целящи ограничаването на идентифицираните и оценени рискове, спрямо които съответното структурно звено трябва да реагира, предвид възприетото ниво на риск-апетита в цялата организация;
- Ръководителите на лаборатории са отговорни да провеждат мониторинг на резултатите от управлението на риска в ръководените от тях звена/дейности. Те докладват резултатите на Риск-ръководителя, който е отговорен за предприемането на по-нататъшни действия. При нужда от предприемане на коригиращи действия, ръководителите на лаборатории участват съобразно компетентността си в тяхното разработване.

2.4. Служители

Служителите на ИФРГ са тези, които прилагат ежедневно контролните дейности, разработени за управление на рисковете. В тази връзка те са в позиция да установят първи евентуални слабости, нередности или проявления на рискове. Отговорностите на служителите са:

- Да подпомагат ръководителите на лаборатории в процеса на управление на риска, като осигуряват нужната за целта информация и участват активно в дейностите по оценка на идентифицираните рискове и въведените контролни процедури;
- Да докладват на Оперативното ръководство за възникващи проблеми, които могат да застрашат постигането на целите;
- Да докладват на Оперативното ръководство за потенциални възможности за подобрене на системите за вътрешен контрол.

II. ПРОЦЕС ПО УПРАВЛЕНИЕ НА РИСКА

1. Идентифициране на рисковете

За целите на текущото идентифициране на рисковете, застрашаващи целите на Организацията, всеки служител, който счита, че е идентифицирал нов риск или промяна във вероятността или влиянието на съществуващ риск, трябва да информира ръководителя на структурното звено, в което работи (риск-собственика). Риск-собственикът преценява дали има основания да информира Риск-ръководителя. Всеки служител трябва да има възможност и трябва да е наясно, че ако има нова информация за рисковете, той може да информира директно Риск-ръководителя, ако обективни причини му пречат да информира и обсъди въпроса с ръководителя на структурното звено. Идентифицирането на риска е първата същинска фаза от процеса по управление на риска. Дейностите по управление на риска следва да сведат до приемливи нива съществените рискове, които биха могли да застрашат постигането на целите на ИФРГ или да повлияят негативно на ефективността, ефикасността и/или икономичността на ресурсите, използвани за постигането на тези цели. Следователно процесът по управление на риска започва с определяне на целите на ИФРГ и на отделните му структурни звена.

1.1. Определяне на целите

Основна предпоставка за ефективното управление на риска е определянето на ясни цели и тяхното разбиране. Правилното идентифициране на рисковете е невъзможно да бъде

извършено, ако в Организацията не е въведен адекватен процес на целеполагане. Целите трябва да бъдат разбрани от всички ръководители и служители в организацията, за да се осигури тяхното постигане чрез изпълнение на конкретни дейности и задачи. Следователно, задължителна отправна точка за идентифицирането на рисковете са целите на ИФРГ, в т.ч. целите и задачите на съответните звена единици в Института, определени в мисията и оперативните планове на всяка структурна единица. Интегрираната рамка COSO 2013 въвежда четири принципа на Управление на риска (принципи 6 - 9 на вътрешния контрол):

Принципи на COSO 2013 (т. 6-9)

- Организацията определя цели с достатъчна яснота, за да позволи идентифицирането и оценката на рисковете, свързани с тях.
- Организацията идентифицира рисковете за постигане на целите си и ги анализира от гледна точка на определяне на подходите и начините за тяхното управление.
- Организацията разглежда възможностите за измами при оценката на риска и тяхното влияние при постигане на целите.
- Организацията идентифицира и оценява промените, които биха могли да повлияят значително на системата за вътрешен контрол.

Колкото по-ясно са определени целите, които следва да бъдат постигнати, толкова по-лесно ще бъдат идентифицирани рисковете, които могат да застрашат тяхното постигане. В тази връзка, всяка поставена цел, която трябва да бъде постигната през годината (включително, когато тя представлява междинен етап от дългосрочен проект), следва да отговаря на изброените по-долу критерии, които представляват насоки за формулиране на ясни, конкретни и измерими цели - концепцията на **SMART** целите, според която целите трябва да бъдат:

Specific - Специфични/конкретни, т.е. да бъдат формулирани точно и ясно определени цели, а не общи такива;

Measurable - Измерими, т.е. целите да могат да бъдат измерени в единици;

Achievable – Достижими, т.е. целите трябва да са постижими с наличните ресурси;

Relevant - Уместни, т.е. трябва да са полезни от гледна точка на разглежданата политика, да съвпадат с общата визия и мисия на организацията;

Time-bound - Своевременни, т.е. да се определи времето, за което ще се постигне съответната цел (да има поставен краен срок).

Целите за всяка структурна единица се определят в оперативен/годишен план, изготвен въз основа на целите, формулирани в Стратегията за развитие на ИФРГ. В оперативния план следва да се дефинират крайните срокове за изпълнението на целите, съответните дейности и отговорните служители, сроковете и отговорности за отчитане на изпълнението. Анализът на напредъка по постигането на целите се извършва на базата на ясно определени индикатори (критерии), съгласно които към крайния срок се определя дали целта е постигната успешно.

1.2. Класификация на рисковете

След като са дефинирани, целите за всяка структурна единица, нейното ръководство и служителите, ангажирани със съответните дейности, са в позиция да идентифицират съществените рискове, които биха могли да възпрепятстват постигането на целите.

Класификацията на рисковете, използвана в БАН, включва четири нива:

- първо ниво е „Риск клас“;
- второ ниво - „Риск категория“;
- трето ниво - „Риск под-категория“;
- четвърто ниво - „Риск“.

Петте основни риск класа са: Управление и надзор, Стратегия и планиране, Оперативна дейност и инфраструктура, Съответствие и Докладване. Категориите, подкатегиите и отделните възможни рискове в рамките на всеки един клас са представени в работен документ - **Карта на риска (Приложение № 1)**. Картата на риска е инструмент, който улеснява идентифицирането на рисковете за всички структури в системата на БАН и предоставя единна рамка за класификация на рисковете. Тя не следва да се разглежда като напълно изчерпателен списък за всички потенциални или приложими за БАН рискове. Изключително важно е на всички нива в БАН и всички служители да използват една и съща терминология за дефиниране на риска. Ако към дадена риск подкатегория се прибави нов риск или се промени дефиницията на вече включен в класификацията риск, ръководителят на съответната структурна единица, която е идентифицирала необходимостта от промяна, е длъжен да обсъди решението си с Комитета по риска, който следва да информира за това всички структури в БАН, с оглед използване на унифициран подход.

1.3. Попълване на риск-регистър

Риск-регистърът служи за документиране на основните етапи и дейности от процеса по управление на риска. Риск-регистърът е документ в установения формат (**Приложение 2) Риск-регистър/Risk Register-BG.xls**), който е еднакъв за всяка самостоятелна структурна единица в системата на БАН.

За всяка от целите на звеното се идентифицират съществените рискове, съгласно класификацията от Картата на рисковете. Всяко структурно звено попълва своя Риск-регистър, като колоните „Категория“, „Подкатегория“ и „Риск“ се попълват съгласно термините в класификацията.

За всеки от идентифицираните рискове се определя номер (Риск ID), който подпомага ориентирането към кой клас спада рискът и кой номер подред е в Риск-регистъра по следната схема:

Клас	Номер	Риск ID
Управление и надзор	1.. ...п	УН1... ...УНп
Стратегия и планиране	1.. ...п	СП1... ...СПп
Оперативна дейност и инфраструктура	1.. ...п	ОДИ1... ...ОДИп
Съответствие	1.. .п	С1... ...Сп
Докладване	1.. ...п	Д1.. ...Дп

В колона „Описание на риска“ всяко структурно звено попълва индивидуалното си разбиране за проявлението на дадения риск конкретно в рамките на структурата и нейните цели/дейности.

Работна група от ръководството и служителите на всяко от структурните звена в ИФРГ е ангажирана да попълни Риск-регистъра за съответното звено. Риск-регистрите на всяко звено се представят от съответния ръководител на структурното звено пред Комитета по риска поне веднъж годишно (в началото на годината), заедно с представянето на целите, описани в годишния/оперативен план на структурата. За самостоятелните единици в системата на БАН попълнените риск-регистри се представят на отговорника по риска, определен от съответния ръководител на структурната единица.

На базата на риск-регистрите на отделните структурни звена и чрез провеждането на работни срещи, Комитетът по риска създава риск-регистъра на ИФРГ, в който идентифицира рисковете, застрашаващи постигането на целите на ИФРГ.

2. Оценка на риска

Поради необходимостта да се отдели сериозно внимание на основните рискове, с които се сблъсква ИФРГ, по принцип не е възможно да бъдат идентифицирани и управлявани повече от 20 - 30 риска на ниво организация/структурна единица. Затова е необходимо вниманието да се концентрира към идентифициране на най-важните (съществените) рискове. Това са тези, за които съществува най-голяма вероятност да настъпят и са с най-

голямо потенциално влияние върху стратегическите и оперативни цели. Основната задача на този етап е рисковете да бъдат анализирани и оценени, за да могат да бъдат определени съществените рискове и да се вземе решение как да се контролират и какво въздействие трябва да бъде оказано върху тях - каква трябва да бъде реакцията на риска. Идентифицираните рискове за всяка структурна единица в системата на БАН се оценяват по показателите „Влияние” и „Вероятност”.

2.1. Оценка на присъщия риск

Оценяват се потенциалното **влияние и вероятност** на присъщия риск, който се дефинира като: „Рискът, съществуващ при липса на всякакви действия, предприети от ръководството за промяна на вероятността или на влиянието на риска”, т.е. оценява се въздействието на риска при липсата на каквито и да е контролни дейности за управлението му. Присъщите рискове следва да се оценяват еднократно, само през първата година от прилагането на Стратегията за управление на риска, както и нововъзникналите рискове. Впоследствие те подлежат на преоценка за евентуални промени в нивото на влиянието и вероятността от възникването им.

ВЛИЯНИЕ

Влияние: Ако този риск възникне, какво ще бъде въздействието му върху постигането на целите ви?

Оценките за измерване на влиянието са представени в таблицата по-долу:

Оценка	Описание
1	Несъществено
3	Малко
5	Умерено
7	Съществено
9	Изключително голямо

Критериите за оценка на влиянието са представени в работен документ „Примерни критерии за оценка на влиянието” (Приложение 3).

ВЕРОЯТНОСТ

Всеки риск трябва да бъде оценен от гледна точка на вероятността рискът да се сбъдне.

Вероятност: До каква степен този риск може да се прояви в настоящето или в обозримо бъдеще (2-3 години)?

Оценката се прави според скалата, описана по-долу:

Оценка	Описание
1	Не е вероятно
3	Рядко
5	Възможно
7	Вероятно
9	Почти сигурно

Като критерии за оценка на вероятността може да се използва реална информация за минали

периоди от време.

2.2. Определяне на адекватността и ефективността на контрола

Адекватните контролни дейности са създадени за минимизирането на определени рискове и са планирани и организирани по начин, който дава разумно ниво на увереност, че целите ще бъдат постигнати ефикасно и икономично. Следователно, адекватните контролни процедури са разположени на точното място, в правилното време и по своята същност могат да допринесат за минимизирането на съответния риск в желаните граници - т.е. дизайнът им е такъв, че ако бъдат прилагани на практика от служителите, целите ще бъдат постигнати. Именно последното условие реферира към ефективността на вътрешния контрол.

Оценката за ефективност представлява отговор на въпроса функционира ли и в каква степен така създадената система за вътрешен контрол. Една контролна процедура може да бъде много подходяща като дизайн (т.е. адекватна), но на практика да не се прилага. Възможен е и обратният вариант - за определена дейност да бъдат стриктно прилагани контролни процедури, които са неподходящи и създадени по начин, който не допринася за минимизиране на рисковете и постигане на целите.

Като част от процеса по управление на риска се определят съществуващите механизми за контрол, които могат да ограничават идентифицираните рискове.

Оценката на ефективността на контрола по същество представлява оценка и на остатъчния риск, който се дефинира като „рискът, който остава след реакцията на риска от страна на ръководството”, т.е. вземат се предвид съществуването или липсата на контроли или други дейности по управлението му.

Оценката на ефективността на контрола се прави чрез следните два показателя:

- **Стойност на риска** - стойността на риска се изразява като средно аритметична величина на влиянието и вероятността (нанася се по вертикалата на графиката)
- **Адекватност и ефективност на контрола** - те определят като отговор на въпроса - До каква степен активно контролирате този риск (каква е възприеманата адекватност и ефективност на дейностите/наличните контроли, които упражнявате)? Стойността на остатъчния риск се определя от адекватността и ефективността на контролите. Колкото по-неадекватни и по-неефективни са контролите, толкова е по-висок остатъчният риск.

Оценката за Адекватност и Ефективност и на контрола се прави според скалата, описана по-долу:

Оценка	Описание
1	Трябва да правим много по-малко
3	Трябва да правим по-малко
5	Усилията, които полагаме за този риск, са напълно адекватни
7	Трябва да направим повече
9	Трябва да направим много повече

- **Висок риск** е този, който се оценява с висока стойност и към който не е приложен адекватен и ефективен контрол.
- **Среден риск** е този, който:
 - 1) е с висока стойност, но са предприети необходимите мерки за ограничаването му чрез въвеждане на адекватни и ефективни контроли. Вътрешният одит следва да даде разумна увереност на Ръководството относно ефективността и ефикасността на контролите или,

2) е с ниска стойност, но организацията е изложена на този риск поради липса на ефективни контролни механизми за ограничаването му, като в този случай следва да се анализира общото въздействие на всички такива рискове, за да се провери дали те не надвишават риск апетита.

- **Нисък риск** е този, който има ниска стойност и същевременно са предприети необходимите мерки за ограничаването му чрез въвеждане на ефективни контролни дейности. Ръководството следва да прецени дали да запази съществуващото ниво на контролни дейности или да преразпредели ресурсите, тъй като поради ниската си стойност този риск би могъл до голяма степен да се приеме.

Риск рейтинг

Математически изразен, остатъчният риск е резултат от стойността на риска и ефективността на контрола. Риск-апетитът на ниво ИФРГ за остатъчен риск е, както следва:

ОЦЕНКА (стойност на риска 1 ефективност на контрола)	РЕЙТИНГ
1-15	ПРИЕМЛИВ
16-54	ИЗИСКВА ВНИМАНИЕ
55-81	НЕПРИЕМЛИВ

3. Попълване на риск-регистър

Индивидуалните оценки в цифри на влиянието и вероятността на всеки идентифициран риск се попълват в Риск-регистъра, който автоматично пресмята стойността на риска. След това се пристъпва към оценка на адекватността и ефективността на контрола, а на база на тази тези две оценки се определя и рейтингът на всеки един от рисковете, отнесен към риск-апетита на ИФРГ.

Членовете на Комитета по риска или съответно работната група за оценка използват попълването на Риск-регистъра като основа за дискусия, чиято цел е постигането на консенсус и общо разбиране за оценката на всеки от идентифицираните рискове. След като се попълни риск-регистърът, резултатите могат да бъдат представени графично.

4. Реакция на риска

След като идентифицираните рискове са оценени, ръководителите на структурните звена след съгласуване с Комитета по риска, вземат решение относно подходящата реакция към всеки от рисковете, като съобразяват решението си с риск-апетита на ИФРГ.

- **Ограничаване на риска** - Ограничаването на риска представлява намаляване или третиране на риска чрез прилагане на контроли (например, чрез законодателството, партньорство и сътрудничество, повишаване на ефикасността на контрола чрез засилване на съществуващите контроли или въвеждането на нови и т.н.) с цел да се намали остатъчният риск. Ограничаването на риска е най-често срещаната реакция, която ръководителите следва да прилагат. Причината за това е, че рискът рядко може да бъде изцяло избегнат/прехвърлен. Ето защо следва да се въведат контролни дейности, предоставящи разумна увереност за ограничаване на риска в приемливи параметри, в зависимост от значимостта на риска и съобразно разходите за въвеждането на контролите. Рисковете, обект на тази реакция, трябва да се наблюдават периодично. Решението да се ограничи даден риск изисква: адекватен подбор на действията в съответствие с оценката на риска; добро разбиране в сферата на вътрешния контрол; внимателно анализиране на разходите и ползите от контрола; дефиниране на

специфични дейности за ограничаване или третиране на риска и ясно определяне на роли и отговорности. Това е най-често предприеманата реакция на риска в публичния сектор.

- **Прехвърляне на риска** - Прехвърляне или споделянето на риска по същество означава да се влезе в партньорство с трета страна, така че той да бъде управляван съвместно. Типични примери за прехвърляне на риска са застраховането, публично-частните партньорства, различни степени на сорсинг споразумения (споразумения на реципрочна основа) и др. Друг способ за прехвърляне на риска е сключването на споразумение с друга организация, по силата на което се прехвърля дейността заедно със съответните рискове, по общо съгласие на страните. Подобни схеми позволяват достъп до допълнителен ресурс (например, контролни дейности или опит и квалификация), като в същото време ограничават възможността от загуба на контрол над дейностите, която е възможна при 100% прехвърляне на трета страна. Ръководителите на структурни звена, Комитетът по риска и Директорът, като цяло продължават да бъдат отговорни лица за управлението на риска, независимо от факта, че рискът е прехвърлен или споделен.
- **Приемане/толерирание на риска** - Такава реакция е възможна, само ако определени рискове имат ограничено (незначително) влияние върху постигане на целите или ако разходите за предприемане на действия превишават потенциалните ползи. Такива рискове, обаче, трябва да бъдат постоянно наблюдавани. Възможно е различни външни или вътрешни фактори да окажат въздействие върху вероятността и влиянието и да изместят риска в друга по-висока категория. Приемането или толерирането на даден риск означава, че Организацията поема риска без да предприеме конкретни мерки за управлението му. Такова решение означава, че Комитетът по риска следва периодично да наблюдава и преоценява риска, за да може при необходимост да бъде избран друг подход за управлението му. Решението да се толерира даден риск трябва да бъде взето, имайки предвид оценката на риска, последствията за постигането на целите, риск-апетита и правните последици (например, решението да не се предприемат действия може да доведе до по-голям риск). Причините да се толерира даден риск без по-нататъшни действия за управлението му могат да бъдат:
 - Рискът има ограничено (незначително) влияние върху постигането на целите на организацията/структурата;
 - Действията по ограничаването на риска са свързани със съществени контролни дейности, разходите за които значително надхвърлят ползите;
 - Поемането на риска е свързано със самото развитие на организацията, т.е. за да постигне целите си, тя трябва да остане гъвкава към променящата се среда, да извършва нови дейности и методи на работа и да търпи развитие, което би било ограничено в контролирана среда;
 - Управлението на риска е извън контрола на ръководството и/или неизлагането на риск би могло да означава преустановяване на дейности, които са от ключова важност за организацията.
- **Прекратяване (избягване) на риска** - Избягването на даден риск означава да се прекратят дейностите, свързани с потенциалното му проявление. Подобно решение би могло да означава, че Комитетът по риска следва да преразгледа поставените цели и доколко те са изпълними и съвместими с останалите цели и основни дейности. Също така Комитетът трябва да разгледа приложимите регулаторни изисквания и ограничения, за да прецени дали е допустимо дадена дейност да не се извършва или да не се оперира в определена среда. Следва да се разгледат и възможности за избягване на риска в определена степен, т.е. дадени цели или дейности да бъдат частично променени или преустановени, както и да се установят възможностите поставените цели да бъдат постигнати по различен от предвидения начин.

4.1. Разработване на контролни дейности

За рисковете, за които ръководителите на структурни звена и/или Комитетът по риска е избрал реакция „Ограничаване“, т.е. прилагане на контрол, се определя съответната цел на контрола. Целите на контрола могат да бъдат:

- **За съответствие със законодателството, вътрешните актове и договори:**

Всички организации от публичния сектор, в т.ч. и БАН функционират в силно регулирана среда и са длъжни да спазват множество закони и подзаконови нормативни актове, както и вътрешни правила и договори. Законосъобразността е основно и първостепенно изискване към дейността на организациите от публичния сектор. При дефинирането на целите, винаги на първо място трябва да се държи сметка за законосъобразността и системите за вътрешен контрол, които следва да са насочени към постигане на пълно съответствие с приложимата нормативна и регулаторна рамка. Ръководителите са длъжни да осигурят спазване от страна на всички служители на приложимото законодателство, вкл. вътрешните актове и договорите, по които те са страни. Те регулират основните процеси и дейности, осъществявани в организациите от публичния сектор, начина на функционирането им, събирането и разходването на публичните средства и др.

- **Надеждност и всеобхватност на финансовата и оперативна информация:**

Ръководителите на организациите организират регистрирането и комуникацията на достатъчна, уместна, надеждна, полезна и своевременна информация. Създаваната, съхраняваната, ползваната и предоставяната от дадена организация информация има както финансов, така и нефинансов характер. Тя е от изключително значение, тъй като е база за изпълнение на задачите, за взимане на решения, както и за изготвяне на верни, точни и честни финансови отчети.

- **Икономичност, ефективност и ефикасност на дейностите:**

Принципът за доброто финансово управление се базира на тези три изисквания.

Икономичност е придобиването с най-малки разходи на необходимите ресурси за осъществяване на дейността на организацията от публичния сектор при спазване на изискванията за качество на ресурсите.

Ефективност е степента на постигане на целите на организацията от публичния сектор при съпоставяне на действителните и очакваните резултати от нейната дейност.

Ефикасност е постигането на максимални резултати от използваните ресурси при осъществяване на дейността на организацията от публичния сектор.

- **Опазване на активите и информацията:**

Придобиването, използването и разпореждането с активите и информацията изискват специални грижи от страна на ръководителите. Изграденият вътрешен контрол трябва да гарантира опазването на активите и информацията и да действа превантивно срещу кражби, злоупотреби, унищожаване и други неправомерни действия. Ръководителите трябва да обърнат специално внимание на опазването на активите и информацията във връзка с развитието на информационните технологии и тяхното прилагане в организациите от публичния сектор. Опазването на определени информационни ресурси и данни става все по-сложно и важно с използването на информационните и комуникационни технологии. Чувствителната информация, съхранявана в компютърна среда, може да бъде унищожена или копирана, разпространена или използвана без правомощия, ако не се направи всичко възможно за опазването ѝ.

- **Предотвратяване и разкриване на измами и нередности, както и предприемане на последващи действия**

ЗФУКПС въвежда понятията нередност и измама, чрез дефинициите за нередност и измама, засягаща финансовите интереси на Европейските общности. Същевременно, измама по националното законодателство е престъпление, наказуемо по Наказателния кодекс, чийто състав има сходства, но и разлики с този на дефиницията по ЗФУКПС. Независимо от разликите в дефинициите, нередностите и измамите са неправомерни действия, които водят до имуществено увреждане на организациите от публичния сектор. В тази връзка,

организациите трябва да разработват и внедряват системи за вътрешен контрол, насочени към предотвратяване, разкриване и коригиране на последиците от измами и нередности. Така дефинираните общи цели на системите за вътрешен контрол може да се допълват, с оглед постигане да определена цел, например целта за повишаване на административния капацитет следва да се постигне чрез законосъобразно придобиване на нужните ресурси, но същевременно следва да се спазват и принципите на икономичност, ефективност и ефикасност.

На базата на избраната реакция на рисковете се определят съответните контролни цели и конкретни контролни дейности, които се вписват в плана за действие (виж по-долу). Броят и обхватът на контролните дейности трябва да е достатъчен, за да даде увереност, че съществените рискове са ограничени до приемливи нива в рамките на риск-апетита на ИФРГ. Контролните дейности трябва да са подходящи, да функционират в съответствие с планираното през съответния период, да са ефективни по отношение на разходите, да са изчерпателни, разумни и свързани с общите цели на организацията.

Контролните дейности/контролите могат да бъдат превантивни, разкриващи или коригиращи и включват например:

- Система за двоен подпис;
- Правила за достъп до активи и информация;
- Предварителен контрол за законосъобразност;
- Политики и процедури за текущ контрол върху изпълнението на поети финансови ангажменти и сключени договори;
- Предотвратяване на измами и нередности. Политики и процедури за последващи оценки на изпълнението;
- Процедури за обективно, точно, пълно, достоверно и навременно осчетоводяване на всички стопански операции;
- Политики и процедури за управление на човешките ресурси;
- Политики и процедури за спазване на лична почтеност и професионална етика;
- Процедури за разрешаване, одобряване и оторизиране;
- Разделение на отговорностите;
- Процедури за наблюдение;
- Общи контроли;
- Механизми за контрол върху приложенията;
- други.

4.2. Дефиниране на специфични дейности за ограничаване или третиране на риска и ясно определяне на роли и отговорности

Мерките, които ще бъдат предприети за ограничаване на всеки от рисковете се комуникират с всички заинтересовани лица под формата на **План за действие**. Комитетът по риска разписва План за действие за ограничаване на рисковете за ИФРГ като цяло, а ръководителите на лабораториите - за съответната структурна единица, за която отговарят. Отговорниците по риска разписват План за действие за ограничаване на рисковете за съответните лаборатории със съдействието на ръководителите им.

Планът за действие има следните характеристики:

- Включва ясно дефинирани отговорности;
- Предвижда постижими, реалистични, прецизни и стриктни крайни срокове за изпълнение;
- Мотивира служителите и създава чувство за лична отговорност и „собственост“ на риска (т.е. определят се канали за комуникация, дейностите се обсъждат, анализират се мнения, предложения и оценки, за да може всеки включен в процеса да е напълно убеден, че дейностите, включени в плана са най-подходящите и най-добрите);
- Определя и разграничава функциите, свързани с ръководството, изпълнението и надзора на дейностите, както и линиите на докладване между тях;
- Позволява лесно и обективно проследяване на напредъка, докладване и отчетност,

като отбелязва етапи на изпълнение и ключови индикатори за измерване на представянето.

Форматът на плана за действие на всяка организационна структура се определя от Комитета по риска. В **Приложение 4** е представен примерен План за действие.

5. Мониторинг и докладване

След като стратегията за отговор на риска е определена, е необходимо постоянно наблюдение с цел да се гарантира, че тя е въведена и работи успешно. Мониторингът (наблюдението) е може би най-важната стъпка от цялостния процес на управление на риска, тъй като осигурява ранно предупреждение за рисковете, които могат да се сбъднат и материализират. Следва да се има предвид, че мониторингът на процеса по управление на риска е част от системата за мониторинг, като един от петте елемента на вътрешния контрол. В този смисъл е формулиран и един от принципите на елемента Мониторинг, въведен с Интегрираната рамка за вътрешен контрол COSO 2013: „Организацията избира, разработва и извършва текущи и/или отделни оценки, за да се установи дали компонентите на вътрешния контрол присъстват и функционират.“ В тази връзка, директорът на ИФРГ и Риск ръководителят/отговорниците по риска трябва да използват всички инструменти, въведени като част от Мониторинга, като елемент на вътрешния контрол, в т.ч. вътрешния одит, за да следят и оценяват ефективността, ефикасността и икономичността на управлението на риска.

С цел да се подпомогне процесът по мониторинг (наблюдение) на рисковете могат да бъдат използвани ключовите индикатори за изпълнение и ключовите риск индикатори, които са подробно описани в **Приложение 2** на Методическите насоки по елементите на финансовото управление и контрол.

Етапът на докладване на резултатите от управлението на риска е от изключителна важност и следва да бъде организиран по начин, който да осигури непрекъсваемост на процеса. Честотата на докладване зависи от оценката на остатъчния риск. Като минимум, докладването се прави на всяко тримесечие. Нивото, до което се докладват рисковете, зависи от естеството на поставената оперативна цел и на рейтинга на риска, пречупен през призмата на риск-апетита на ИФРГ.

Рискове, дефинирани в риск класове „Управление и надзор“, „Стратегия и планиране“ и „Съответствие“:

- **Всички рискове с оценка на остатъчен риск от 54 или повече** трябва да бъдат докладвани на Комитета по риска.
- **Всички рискове с оценка за влиянието от 7 или повече** трябва да се докладват на Комитета по риска - изисква се потвърждаване, че контролите са налице и че функционират ефективно.

Рискове, дефинирани в риск класове „Оперативна дейност и инфраструктура“ и „Докладване“:

- **Всички рискове с оценка на остатъчен риск от 15 или повече** трябва да бъдат докладвани на ръководителите на звената.
- **Всички рискове с оценка за влиянието от 5 или повече** трябва да се докладват на началниците на ръководителите на звената - изисква се потвърждаване, че контролите са налице и че функционират ефективно.
- В резултат на извършения преглед се изготвя доклад, който се изпраща за информация на Комитета по риска.

Форма и съдържание на докладите

Целта на тази стратегия не е да опише в детайли формата на докладването, а да посочи минималните изисквания по отношение на това какво трябва да се докладва за всеки риск.

Тези минимални изисквания са:

- Ясно описание на риска, включително на контекста на риска;
- Целта, над чието постигане влияе;

- Оценката на влиянието, вероятността, стойността на риска, рейтинга и на остатъчния размер на риска;
- Съществуващи контроли за отговор на риска;
- Предложената стратегия за намаляване на остатъчния риск с допълнителни действия/контроли;
- Собственик на риска.

Заседанията на Комитета по риска се организират:

- **в началото на годината**, когато се потвърждават целите на отделните звена и се стартира процесът по идентифициране и оценка на рисковете за звената в ИФРГ;
- **среща за оценка на риска**, на която се представят риск-регистрите на всяко звено и се попълва риск-регистъра на ИФРГ;
- **среща за утвърждаване на плана за действие** за управление на идентифицираните рискове (**не е задължително за първата година!**);
- **веднъж на шестмесечие** за полугодишна актуализация на оценката на риска и преглед на плана за действие за постигане на увереност, че усилията са актуални за ситуацията;
- **среща при внезапно възникнала необходимост** в случай на непредвидени обстоятелства или внезапен развой на събитията и т.н.;
- **среща в края на годината за отчитане на резултатите**, на която Комитетът по риска подготвя годишен доклад до Директора, в който отчита дейностите си по управление на риска през годината, както и постигнати цели. Докладът съдържа и становище за цялостния рисков профил на Института и планирани дейности за следващата година.

Примерен календар на срещите на Комитета по риска е представен в Приложение 5.

III. УПРАВЛЕНИЕ НА ЗНАНИЕТО

1. Единна база данни за управление на риска

За да се постигне приемственост в процеса по управление на риска и осведоменост на всички нива в ИФРГ, Комитетът по риска следва да поддържа единна база данни за управлението на риска, в която да се поддържат следните документи в електронен формат:

- актуалната версия на Стратегията за управление на риска;
- изготвени документи с пряко отношение в процеса по управление на риска (документи, свързани с целеполагането, риск-регистри, планове за действие и др.);
- решения и меморандуми от заседания на Комитета по риска;
- политики и процедури, свързани с вътрешния контрол;
- доклади на Комитета по риска;
- други.

Комитетът по риска следва да определи администратор на базата данни, както и правила за достъп до информацията, която се поддържа в нея. Базата данни следва да бъде достъпна за всички служители на ИФРГ (съгласно определените правила и нива на достъп).

2. Регистър на проявилите се рискове

Комитетът по риска поддържа отделен регистър на рисковете, които са настъпили. Целта на този документ е да се осигури обмяна на опит и знания, както във времето, така и между различни служители, за да се подобри ефективността на процеса по управление на риска като цяло.

Форматът на Регистъра на проявилите се рискове позволява:

- да се води история на рисковете, като се посочва дата на проявление на риска;
- да се посочи собственикът на риска (и други отговорни лица за дейностите по управлението му);
- да се опише ситуацията, довела до събъждането на негативното събитие (причините);
- да се опише конкретното проявление на риска и последиците от това (количествени и качествени показатели за последиците);
- да се посочи дали рискът е бил идентифициран и оценен в рамките на редовните заседания за оценка и актуализация на оценката на риска или идентифициран преди

- да се прояви;
- да се посочи предварително определената реакция на риска (включително да се реферира към планове за действия и други свързани документи);
- да се анализира кои от предвидените дейности за ограничаване на риска са били неуспешни и са създали предпоставка за проявление на риска;
- да се посочат сценариите за възможни действия и направения избор, като се подчертаят последващи дейности за ограничаване на риска (включително фактори за успех от плана за възстановяване);
- срок; статус на риска (проявлението е започнало, приключило, води до други рискове, овладяно и др.); статус на изпълнение (дейностите не са започнали, са в процес, завършени).

Комитетът по риска определя отговорно лице, което да поддържа регистъра.

Примерен формат на регистъра на проявилите се рискове е представен в **Приложение 6**.

ПРИЛОЖЕНИЯ:

Приложение 1: Класификация на рисковете

Приложение 2: Риск-регистър

Приложение 3: Примерни критерии за оценка на влиянието

Приложение 4: Примерен формат на план за действие

Приложение 5: Примерен календар на заседанията на Комитета по риска

Приложение 6: Примерен формат на Регистър на проявили се рискове

Приложение 1

КЛАСИФИКАЦИЯ НА РИСКОВЕТЕ

КАРТА НА РИСКОВЕТЕ

в Институт по физиология на растенията и генетика към Българска академия на науките

I. РИСК КЛАС - УПРАВЛЕНИЕ И НАДЗОР

Управлението и надзорът са съвкупност от взаимоотношения и дейности, чрез които се определят целите на организацията и средствата за постигане на тези цели, както и мониторинг на контролната среда.

Това включва:

- Честни и справедливи практики;
- Прозрачност;
- Отчетност.
- Рискове, свързани със структурата, политиката, процедурите и органите, чрез които основните направления и решения на организацията се наблюдават и управляват.

„Корпоративно управление и надзор" и „Етика" са двете категории риск в рамките на този клас.

A. РИСК КАТЕГОРИЯ - КОРПОРАТИВНО УПРАВЛЕНИЕ И НАДЗОР

Корпоративното управление и надзор е съвкупността от процеси, политики, нормативни документи и институции, които влияят на начина, по който организацията е ръководена, управлявана или контролирана. Ключовите елементи на доброто корпоративно управление включват честност, доверие и почтеност, откритост, фокусиране над изпълнението, отговорност и отчетност, взаимно уважение и ангажираност към организацията.

В частност, корпоративното управление подчертава, че Ръководството на организацията трябва да се държи честно и морално, най-вече когато се отнася за действителни или привидни конфликти на интереси и за информацията във финансовите отчети.

Подкатегория - Ефективност на ръководството/управление на знанието Рискове:

- Неразбиране на ръководството относно законово-определените му отговорности или невъзможност да изпълнява отговорностите си;
- Неефективни работни групи;
- Лоша комуникация от страна на ръководството;
- Недостатъчно или липса на знание относно отговорностите на ръководството;
- Недостатъчна комуникация с ръководството;
- Липса на сплотеност на Ръководния състав.

Подкатегория - Структура и лидерски умения. Рискове:

- Липса на подходящи насоки/тон на върха от ръководството;
- Слаба структура/спойка/състав на ръководството;
- Неефективна комуникация между оперативното и изпълнителното ръководство;
- Конфликт на интереси и липса на независимост;
- Неправилно взимане на решения/неподходящ процес по взимане на решения и неподходящо делегиране на правомощия;
- Лоша координация и несъобразяване на дейностите с целите на организацията;
- Невнимание, липса на фокус и усилия над стратегията и изпълнението ѝ.

Подкатегория - Компенсация и възнаграждение / допълнителни стимули, обвързани с представянето. Рискове:

- Неадекватно разкриване/оповестяване/разгласяване на процеса и принципите за компенсация на ръководния състав;

- Показателите за измерването на представянето и изпълнението на дейностите не са съобразени с дългосрочната стратегия;
- Възнаграждението не е съобразено с очакванията на заинтересованите лица;
- Несъобразено голямо/непропорционално внимание и значение на краткосрочни резултати;
- Несъответствие между стимули и възнаграждения.

Подкатегория - Репутация и връзки със заинтересованите лица. Рискове:

- Неспособност да бъдат разбрани и удовлетворени очакванията на служителите, партньорите, обществото;
- Неспособност да бъдат идентифицирани и разбрани тенденции и процеси, свързани със служителите, кредиторите, гражданите и други заинтересовани лица;
- Реално или привидно съществено вмешателство и влияние от страна на външни за организацията лица или обществени/политически групи;
- Неспособност или нежелание да се отговори, да се вземат предвид предложения на служителите и други заинтересовани лица;
- Негативно мнение и лоша репутация на отделни структури, звена, или на организацията като цяло.

Подкатегория - Корпоративна отговорност и устойчивост. Рискове:

- Невъзможност да изпълнят задълженията свързани със социалната отговорност;
- Неспособност да се разберат тенденциите свързани с работната сила на организацията, кредиторите, (взаимоотношения с бизнеса, с обществото, държавните институции) и другите заинтересовани лица.

Подкатегория - Надзор на риска. Рискове:

- Неадекватен надзор над риска, поет от ръководството при изпълнение на дейностите;
- Неподходяща структура, която да позволява единен подход при управлението на рисковете в организацията;
- Неподходящи/неприемливо високи или ниски нива на риск апетит и нива на толериране на риска;
- Липса на риск-интелигентно взимане на решения; решенията се взимат без адекватно да се вземат предвид всички свързани рискове;
- Неподходящо публично оповестяване на високо-рискова информация;
- Неправилно използване или липса на подходяща рамка за управление на риска.

Подкатегория - Прозрачност и финансова отчетност. Рискове:

- Незадълбочен/повърхностен преглед на финансовите отчети и друга свързана информация;
- Неспособност да се поставят под въпрос решенията и мнението на ръководството;
- Неподходящ надзор над вътрешните и външните одитори (финансови контролори);
- Липса на финансова компетентност на оправомощените длъжностни лица по управлението на риска, ръководството и др.

В. РИСК КАТЕГОРИЯ - ЕТИКА

Програмата за етика и съответствие поддържа целите на организацията и определя границите на законно и етично поведение. Утвърждава система за предупреждение на висшето ръководство, когато организацията се приближава до (или пресича) даден лимит или се сблъсква с пречка (например злоупотреба, вътрешни измами, несъответствие, неетично поведение и т.н.), която влияе негативно на постигането на целите.

При невъзможност за ефективно съставяне и изпълнение на програма за етика и съответствие, организацията не може да насърчи култура на доверие, отчетност и/или почтеност. Възможни са действия свързани с измама или злоупотреба.

Организацията трябва да вгради в своите дейности процесите по етика и съответствие

при управление на риска и да поощри служителите да сигнализират при нарушения на съответните стандарти.

Подкатегория - Подход в отговор на обвинения. Рискове:

- Проучвания, обвинения, твърдения и др. не се документират; не се документират резултатите и предприетите действия;
- Липса на дефинирана, формална процедура при криза;
- Загуба на чувствителна информация поради безотговорно/неподходящо боравене/съхранение с нея.

Подкатегория - Комуникация и докладване. Рискове:

- Липса на текуща комуникация относно въпроси, свързани с етичния климат;
- Липса на подходящи методи, чрез които служителите могат да повдигат въпроси свързани с етиката;
- Липса на анонимна линия за докладване;
- Неспособност да се създаде ангажираност у служителите и етично самосъзнание, както и възприемането на етиката като въпрос от първостепенна важност;
- Неспособност да бъдат идентифицирани и докладвани тенденции, свързани с етиката;
- неподходящи източници за докладване на етични нарушения;
- неподходящо докладване на съществени етични нарушения към съответните външни заинтересовани лица.

Подкатегория - Корективни действия и дисциплина. Рискове:

- Неспособност да бъдат наказани служителите в случай на неспазване на правилата;
- Непоследователност на дисциплинарните мерки в случай на неспазване на правилата;
- Неспособност да се комуникират последствията от неетично поведение и неспазване на правилата.

Подкатегория - Етична култура/Тон на върха. Рискове:

- Неспособност да се насърчава етична култура;
- неподходящи стимули за действие;
- Неспособност да се наблюдават и контролират неоторизирани действия;
- Неспособност да се защитават подалите сигнал (whistleblowers).

Подкатегория – Разследване. Рискове:

- Липса на дефиниран протокол за провеждане на разследвания;
- Неспособност да се определят и оценят рискове, свързани с етичния климат;
- Неспособност да се определят процесите и действията, повлияни от рисковете свързани с етиката.

Подкатегория - Мониторинг и одит. Рискове:

- Неспособност за провеждане на рутинни одити на съответствието;
- Неуместно разпределение на ресурсите за мониторинг и одит;
- Неспособност непрекъснато да се наблюдават етичния климат в структурите на организацията.

Подкатегория - Структура и надзор. Рискове:

- Неадекватна структура на надзора;
- Неуместна политика на надзора;
- Неуместно делегиране на отговорности и последващ мониторинг на действията.

Подкатегория – Обучение. Рискове:

- Неадекватна програма за обучение по етика и съответствие;
- Неспособност да се обучат характерни структурни единици по политиките и

- процедурите на етика и съответствие;
- Неспособност да се проследи изпълнението на обучението.

II. РИСК КЛАС - СТРАТЕГИЯ И ПЛАНИРАНЕ

Стратегията и планирането включват стратегическите решения на организацията за изпълнението на целите ѝ.

Разглеждането на риска като фактор при развиването на стратегията на организацията може да помогне за:

- Идентифициране и приоритизиране на проблемните области;
- Подготвяне на стратегически план за действие с ясно дефинирани отговорности и отчетност, резултати и крайни срокове.

Планирането осигурява детайлна и логична рамка за постигане на стратегическите цели на организацията.

A. РИСК КАТЕГОРИЯ - СОЦИАЛНА ОТГОВОРНОСТ И УСТОЙЧИВОСТ

Тази категория риск се отнася до непрекъснато подобряване на дейността за гарантиране наличност на ресурсите в дългосрочен план чрез прозрачно и социално ориентирано отношение към околната среда.

Подкатегория - Обществени инвестиции. Рискове:

- Недостатъчни обществено значими инициативи;
- Липса на вътрешна подкрепа за развитие на обществените начинания;
- Неефективно докладване на обществените инвестиционни начинания;
- Неефективни решения и програми за аутсорсване в чужбина (по-евтини дестинации) на дейности и производства;
- Липса на достъпност за възрастни и хора с увреждания.

Подкатегория - Управление на енергията и достъп до алтернативни източници Рискове:

- Неадекватна икономия на енергия;
- Невъзможност да се използват алтернативните източници на енергия;
- Несъответствие на използването и икономията на енергията със съответните закони и регулации.

Подкатегория - Взаимодействие с бизнеса. Рискове:

- Липса на подходящо законодателство;
- Незаинтересованост на бизнеса от дългосрочни инвестиции в науката;
- Липса на достатъчно ефективни посреднически звена наука-бизнес;
- Неспособност да се приемат добри търговски бизнес практики;
- Неспособност да бъдат сертифицирани продукти;
- Неспособност да се постигне растеж и репутация чрез честна търговия.

Подкатегория - Използване и осчетоводяване на природни ресурси. Рискове:

- Стоков риск и защита на природните ресурси;
- Невъзможност да се облекчи зависимостта от природните ресурси;
- Неадекватни системи и процеси за отчет и използване на природните ресурси.

Подкатегория - Благотворителност. Рискове:

- Недостатъчни благотворителни дейности;
- Неспособност да се насърчат служителите в сферата на благотворителността;
- Неефективен отчет на благотворителните дейности.

Подкатегория - Финансиране на проекти. Рискове:

- Финансиране на проекти с вреден ефект върху природата;

- Неспособност да се наблюдава общото финансиране на проекти;
- Финансиране на проекти, нарушаващи човешките права.

Подкатегория - Стратегии за устойчиво развитие. Рискове:

- Неспособност да се демонстрира корпоративна и социална отговорност;
- Лоша устойчивост при изпълнение на основни дейности и процеси.

Подкатегория - Намаляване на отпадъците и затворен цикъл на производство. Рискове:

- Неспособност за намаляване на отпадъците;
- Неправилни практики за третиране, повторна употреба и изхвърляне на отпадъците;
- Неспособност да се приеме устойчив процес на производство;
- Несъответствие с приложимите закони и регулации за управление на отпадъците.

В. РИСК КАТЕГОРИЯ - ВЪНШНИ ФАКТОРИ

Външните фактори, като политически, икономически, пазарни, социални, технологични, правни, регулаторни, свързани с измами, условия и околната среда, биха могли да представляват заплаха за организацията. Проявлението на тези фактори не може да бъде контролирано от организацията, но те се случват достатъчно регулярно, за да бъдат до голяма степен предвидими.

Подкатегория – Конкуренция. Рискове:

- Неадекватен анализ на конкуренцията;
- Антимонополни действия;
- Липса на посредничество.

Подкатегория - Икономически условия/Секторни и браншови тенденции. Рискове:

- Промени в макроикономическата среда;
- Демографски промени;
- Инфлация/дефлация;
- Фискални политики (вътрешни и на чуждестранните партньори).

Подкатегория – Измами. Рискове:

- Измама от страна на външни лица;
- Измама от страна на трети страни като доставчици, публични и частни партньори и др.;
- Неефективни програми, целящи предотвратяване, идентифициране и действия за елиминиране на измами.

Подкатегория - Геополитически. Рискове:

- Политическа нестабилност;
- Влошаване на дипломатически и търговски отношения;
- Корупция/корупционен риск.

Подкатегория - Кризи/катастрофи/бедствия. Рискове:

- Епидемии (например коронавирус, свински грип, птичи грип);
- Природни бедствия;
- Аварии;
- Катастрофи, причинени от човешка грешка;
- Тероризъм.

Подкатегория - Закони и регулации. Рискове:

- Лобизъм;
- Негативни нормативни промени, регулации с негативен за страната/дейността на организацията ефект;
- Неспазване на приложимото международно законодателство.

Подкатегория - Финансов/пазарен риск. Рискове:

- Финансов пазарен риск;
- Ценови риск (цени на суровини/стоки);
- Риск, свързан с лихвените проценти;
- Валутен риск.

Подкатегория - Трети страни/партньорства/съвместни проекти. Рискове:

- Финансиране на проекти;
- Договорен риск;
- Незачитане/слабо зачитане на трудовите и човешките права.

С. Риск категория - Планиране

Осигурява подробна, логична рамка за постигането на стратегическите цели на организацията. Процесът на организацията за дефиниране на стратегията чрез изпълними действия (а не общи термини) и взимане на решения за разпределяне на ресурсите за постигане на тази стратегия.

Осъществяването на планове се случва с адекватната подкрепа на ръководството, служителите и другите заинтересовани лица.

Рискове свързани с планирането:

- Невъзможност за синхронизиране на функционалните стратегии и цели по-общите стратегии/стратегия на организацията;
- Неефективно планиране, което може да доведе до грешно разпределение на ресурсите, нерентабилни дейности, проекти или операции.

Подкатегория - Капиталово планиране. Рискове:

- Недостъпност до финансиране;
- Неуместна капиталова структура и съотношение на кредит спрямо собствени средства, структура на финансирането;
- Инвестиционен риск;
- Риск от разпределението на капитала;
- Неспособност да се синхронизират стратегическите цели с капиталовото планиране.

Подкатегория - Планиране на оперативната дейност. Рискове:

- Не се изготвят оперативни планове в отделните структурни звена;
- При планирането на цялостната дейност на организацията не се взимат предвид отделните дирекции/звена;
- Изготвените и поставени планове не са съобразени със стратегията за развитие на организацията и съответно не са изпълними;
- Неподходящо използване на ресурси.

Подкатегория - Измерване на представянето. Рискове:

- Неспособност да се измерва представянето;
- Липса на ключови показатели за измерване на представянето (KPIs);
- Неподходящо комуникиране/разясняване на очакваното представяне и цели;
- Неодобрение/невъзприемане и неизползване на основни/стандартни показатели за измерване на дейността.

Подкатегория - Планиране на сценарии. Рискове:

- Не се планират различни сценарии при дългосрочното планиране;
- Не се вземат предвид основни фактори и критерии, които определят вариации в сценария/сценариите;
- Неподходящи действия спрямо сценариите.

D. РИСК КАТЕГОРИЯ - СТРАТЕГИЯ

Стратегията включва планиране на действията на организацията в дългосрочен план за постигане на целите ѝ. Ръководството трябва да вземе предвид риска при формулирането на стратегията. Този подход помага при идентифициране и приоритизиране на проблемните области и подготвяне на стратегически план за действие с ясно дефинирани отчетност, резултати и крайни срокове.

Подкатегория - Съюзи и партньорства. Рискове:

- Неспособност да се идентифицират възможности за партньорство;
- Неподходящ и недостатъчен анализ на взаимовръзките и отношенията с партньорите;
- Неуспех при дефинирането на обхвата и границите на партньорството;
- Лош мониторинг и управление на партньорските връзки;
- Лош, неподходящ процес за разрешаване на спорове.

Подкатегория – Растеж. Рискове:

- Неефективна стратегия за развитие и комуникация;
- Неспособност да се определят възможностите за растеж.

Подкатегория – Пазари. Рискове:

- Риск на финансовите пазари;
- Недостатъчно внимание към външните фактори.

Подкатегория - Сливания/придобивания/продажби. Рискове:

- Неспособност да се определи ясна крайна визия за интеграция;
- Недостатъчно наблюдение на счетоводните, данъчни, регулаторни и оперативни цели.

Подкатегория – Политики. Рискове:

- Неподходящо комуникиране на политиките;
- Неефективно внедряване, утвърждаване на политиките;
- Политиките си противоречат или противоречат на оперативната дейност и цели.

Подкатегория - Прехвърляне на дейности на външни организации. Рискове:

- Загуба на контрол и отговорност, особено над основни дейности и функции;
- Прекомерна зависимост от трети страни;
- Неспособност да се осъществява мониторинг и проверка на външните организации;
- Липса на специфични критерии за избор на партньор и качество на осъществяваната от него дейност.

Подкатегория - Визия, мисия и ценности. Рискове:

- Неспособност да се артикулира визия, която да вдъхновява и мотивира цялата организация;
- Неуспех при дефинирането на мисия на организацията;
- Неуспех при дефинирането и установяването на ценности, които да са общи за всички в организацията.

Подкатегория – Технологии. Рискове:

- Неспособност да се планира правилно излизането от употреба на дадена технология;
- Неспособност да се прилага технологията;
- Неефективно/забавено развитие, тестване и въвеждане на нови технологии.

III. РИСК КЛАС - ОПЕРАТИВНА ДЕЙНОСТ И ИНФРАСТРУКТУРА

Този клас рискове може да включва случаи на загуби, произтичащи от неадекватни или неуспешни вътрешни процеси, хора и системи, неизправност на инфраструктурата свързана

с изпълнение, защита и използване на съществуващи активи. Чрез фокусиране над настоящите процеси/инфраструктури и техния принос за постигането на целите на организацията и интегрирането на управлението на риска в основните оперативни дейности, организацията може да предотврати ненужни процедури и разходи.

Краткосрочните и дългосрочните оперативни нужди трябва да бъдат определени и планирани така, че да се осигури предлагане и конкурентна структура на разходите, както и стратегическо и ефективно управление на тези критични фактори.

А. РИСК КАТЕГОРИЯ - УПРАВЛЕНИЕ НА АКТИВИТЕ

Активите включват, както материални активи (имоти, машини, оборудване и съоръжения), така и нематериални активи (интелектуална собственост, човешки капитал на организацията.)

Неспособността да се предпазят активите от рискове, свързани с околната среда (наводнения, земетресения) и рискове свързани с достъп (неразрешено влизане, щети и незаконно присвояване), както и невъзможността да се осигури безопасността на човешкия ресурс/капитал водят до загуба на активи.

Неефикасното използване и неадекватната поддръжка на активите могат да доведат до неефективна работа. С нарастващия акцент над въздействието и устойчивостта на околната среда, проектирането на съоръжения и оборудване трябва да вземе под внимание и ефикасното потребление и отделяне екологични/замърсяващи материали и процеси.

Подкатегория - Сгради и оборудване. Рискове:

- Несъответствие между финансовата и физическата информация;
- Неадекватно застрахователно покритие;
- Неспособност за употреба на оборудване, което използва възобновяеми или алтернативни източници на енергия;
- Неспособност за извеждане от експлоатация на съоръжения и възстановяване на сгради, използвайки най-добрите решение за околната среда.

Подкатегория - Нематериални активи. Рискове:

- Нарушение на авторските права/марката;
- Липса на трудови договори;
- Кражба на интелектуална собственост;
- Непълноценно използване на нематериалните активи.

Подкатегория - Лична безопасност. Рискове:

- Неподходящи условия на лична безопасност;
- Липса на адекватни процеси за периодичен преглед, комуникация и утвърждаване на политиките за здраве и безопасност;
- Неспазване на приложимото законодателство.

Подкатегория - Физическа сигурност. Рискове:

- Неуспешно/неефективно внедряване на контроли, осигуряващи сигурността;
- Неподходящи процеси и политики, които да осигурят сигурността на физическите активи;
- Неефективни планове за ограничаване на риска за физическата сигурност;
- Кражба.

Подкатегория - Управление на процесите. Рискове:

- Неспособност да се проследяват активите и свързаната с тях информация;
- Неподходяща логистика;
- Неефективни и неефикасни процеси.

Подкатегория – Данъци. Рискове:

- Прекомерни данъчни оценки на имотите;

- Неспособност да се намалят данъчните разходи свързани с придобиване на материални активи и съоръжения;
- Неоптимизирана политика на амортизация.

Подкатегория - Използване и оползотворяване. Рискове:

- Неправомерно разпореждане с, използване или присвояване;
- Ненавременни, закъснели дейности по поддръжка и ремонт;
- Недобро планиране на капацитета и оползотворяването;
- Неподходящи локации;
- Неефективно използване.

В. ФИНАНСИ

Финансите са свързани с набавянето, разпределението и използването на парични средства, както и с инструментите и анализите, нужни за взимането на тези решения. Основната цел на функцията „Финанси“ е да увеличи стойността на организацията и да се намалят финансовите рискове. Организациите са изложени на финансови рискове в следните области: структура и разпределение на капитала, финансова информация, валутни курсове и др.

Подкатегория – Счетоводство. Рискове:

- Неподходяща счетоводна политика;
- Недостатъчен контрол на записите в главната книга;
- Липса на цялост на финансовата информация;
- Липса на знания за счетоводните принципи и практики;
- Недостатъчни програми и контрол срещу измами;
- Неподходящо/неадекватно управление на предварителни разчети и резерви.

Подкатегория - Качество на одита. Рискове:

- Неспособност да се оцени ефективността на вътрешния контрол;
- Неспазване на управленските решения и контрол;
- Прекомерна зависимост от работата на другите;
- Неефективно планиране и управление на вътрешния одит.

Подкатегория - Управление на капитала. Рискове:

- Неправилно капиталово бюджетиране;
- Загуби при изплащане на дългови задължения;
- Неспособност за оценка на оптималните финансови източници и разходи.

Подкатегория - Инвестиции във финансови активи. Рискове:

- Неподходяща информация за инвестиционни решения;
- Неспособност да се балансира инвестиционното портфолио;
- Липса на ефективен екип за управление на инвестициите.

Подкатегория – Застраховки. Рискове:

- Неподходящо покритие на застраховките;
- Липса на оценка на покритието на застраховките;
- Неспособност за мониторинг на своевременно докладване.

Подкатегория - Планиране/Бюджетиране/Прогнозиране. Рискове:

- Неточна информация използвана в процеса на планиране и бюджетиране;
- Неспособност за мониторинг на плановете и бюджета.

Подкатегория – Данъци. Рискове:

- Неадекватно или прекалено агресивно данъчно планиране;
- Неспособност да се изпълнят данъчните изисквания;

- Неадекватно управление на данъчния риск;
- Неочаквани парични данъци;
- Неспособност да се оптимизират данъчните спестявания от бизнес взаимоотношенията.

С. РИСК КАТЕГОРИЯ - ЧОВЕШКИ РЕСУРСИ

Възможните рискове могат да бъдат причинени от слабости или неуспехи на политиките, процесите, практиките и системите, свързани с управлението на човешкия ресурс в организацията. Това включва неадекватна култура, планиране и обучение, подпомагащи процеси, системи и рамки, ангажменти към и в подкрепа на служителите и ръководството на организацията преди, по време на, при приключване и след официалната обвързаност с организацията.

Подкатегория - Организационна култура. Рискове:

- Лошо изпълнен процес по управление на промяната;
- Нечувствителност към морала на служителя;
- Несъответствие между организационната култура и организационната стратегия;
- Неадекватна комуникация от висшето ръководство.

Подкатегория - Здравеопазване и социални помощи. Рискове:

- Неадекватни помощи за служителите и планове на здравеопазване;
- Несъответствие със счетоводните стандарти и регулации.

Подкатегория - Политики и процедури касаещи човешките ресурси. Рискове:

- Неадекватни трудови стандарти;
- Нарушения в трудовите практики;
- Неспазване на справедливи трудовиотношения;
- Липса на комуникация и обучение по трудовите стандарти.

Подкатегория - Последствия от важни събития. Рискове:

- Трудови протести/стачки, профсъюзи и синдикати;
- Неефективна промяна в управлението;
- Недостатъчни предварителни проучвания в човешките ресурси;
- Организационна несигурност, която води до проблеми с наемането и задържането на кадри;
- Неясни стратегии за комуникация и промяна в управлението.

Подкатегория - Структура на организацията. Рискове:

- Неясно разпределение на правомощията;
- Злоупотреба с правомощията;
- Неподходящо делегиране на правомощията;
- Неподходящо разпределение на правомощията по взимане на решения;
- Сложно устройство/структура на организацията.

Подкатегория - Възнаграждения/заплати. Рискове:

- Неточна обработка на заплатите;
- Неефективна обработка на заплатите;
- Неадекватно разпределение на права и задължения.

Подкатегория - Управление и компенсация. Рискове:

- Неразумни очаквания за представяне;
- Стимулите не са в съответствие с представянето;
- Неефективен контрол/управление на процеса по обезщетение;
- Потенциални измами;

- Неефективен процес по управление на собствения капитал и на отсрочените възнаграждения.

Подкатегория - Развитие на таланти/набиране на персонал. Рискове:

- Липса на приемственост;
- Неефективна политика за задържане на служителите;
- Неспособност да се привлекат и задържат служители;
- Липса на многообразие в работната сила;
- Неефективен процес за набиране на служители;
- Неефективно планиране на работната сила.

Подкатегория - Обучение и развитие. Рискове:

- Неефективни програми за обучение и развитие;
- Липса на подходящи програми за продължителна заетост на служителите;
- Програмите за обучение и развитие не са съобразени с целите и оперативната дейност;
- Аутсорсинг на функцията, занимаваща се с обучение и развитие.

D. РИСК КАТЕГОРИЯ - ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Използването на технологии във всички икономически и обществени начинания създава критична зависимост от ИТ за инициирането, записването и управлението на повечето аспекти, свързани с икономически трансакции, информация и знания.

ИТ рисковете се свързват с неспособността на ИТ да подпомагат мисията, визията и целите на организацията, да бъдат ефективни и ефикасни, да отговарят на правните и екологичните изисквания, както и на изискванията, свързани с качеството и сигурността, да подпомагат докладването и да управляват промените. ИТ рисковете също така включват неефективно управление на продължителността на дейността и планове за реакция след бедствия, лоша архитектура и оперативна неефективност.

Подкатегория – Архитектура. Рискове:

- ИТ архитектурата не е съобразена с целите и стратегията;
- Неспособност да се внедри подходяща технология в подкрепа на целите и стратегията;
- Неспособност да се развие архитектура, която отговаря и поддържа дейностите и процесите;
- Не се взимат предвид промени в дейността и структурата;
- Системите не отговарят на изискванията;
- Неефективна методология за придобиване на софтуер.

Подкатегория - Управление на активи. Рискове:

- Използване на непозволен или нелицензиран софтуер/хардуер;
- Неподходящо/неправомерно управление на наличния софтуер/хардуер;
- Неспособност да се следи работата и наличността на необходимите ресурси.

Подкатегория - Управление на продължителността на бизнеса. Рискове:

- Неспособност да се възстановят данните;
- Критично важни ресурси не са на разположение/липсват;
- Неподходящо планиране за случаи на критични прекъсвания в инфраструктурата;
- Неспособност за възстановяване на основни процеси и дейности.

Подкатегория - Управление на промяната. Рискове

- Неефективни процеси свързани с контрола над промяната;
- Неправомерни/неоторизирани промени;
- Недостатъчно тестване преди имплементацията;
- Невъзможност да се възстанови обработването (processing);

- Неизпълнение на пост-ратифицирана проверка.

Подкатегория - Договаряне и аутсорсинг. Рискове:

- Неправилен процес по искане на оферти и избор на доставчици, договаряне и мониторинг;
- Слаби контроли над сигурността и конфиденциалността на данните;
- Договорни клаузи, които правят невъзможен прегледа на практиките, свързани със сигурността и конфиденциалността.

Подкатегория - Информационна сигурност. Рискове:

- Неефективни/неефикасни контроли на достъпа;
- Уязвимост на външни атаки;
- Неефективна антивирусна стратегия;
- Ненавременно прилагане на „кръпки“ в сигурността;
- Липса на физическа/логическа сигурност;
- Неправилно/липса на разпределение на отговорностите.

Подкатегория – Операции. Рискове:

- Неосигуряване на график на процесите и навременно приключване на процесите;
- Неефикасни процеси и инструменти за запазване на данните;
- Критични данни не се архивират в помещения извън сградата;
- Неспособност да се осигури преносима медия;
- Неспособност да се установят изискваната данъчна и правна информация.

Подкатегория - Конфиденциалност и защита на данните. Рискове:

- Неоторизиран достъп до лични данни;
- Неясна собственост и класификация на данните;
- Липса на интегритет на данните.

Подкатегория - Управление на проблеми. Рискове:

- Ненавременна детекция и докладване на проблеми;
- Неподходящи или ненавременни действия за разрешаване на проблемите;
- Неспособност да се разрешават проблеми.

Подкатегория - Управление на проекти. Рискове:

- Напредъкът по изпълнение на проектите не се проследява, комуникира и докладва;
- Неспособност да се получи одобрение и убеждение у заинтересованите лица;
- Неспособност да се идентифицират, приоритизират, докладват и управляват целите на проекта.

Подкатегория – Записи. Рискове:

- Неподходящо управление на записите;
- Неспособност да се осигури и поддържа сигурността на записите;
- Неспазване на приложимите изисквания;
- Липса на политики и процедури за запазване на данните.

Подкатегория - Лицензиране на технологии. Рискове:

- Неспособност да се импортира/експортира технология, софтуер, данни и/или хардуер;
- Неспазване на законовите изисквания;
- Приложимото законодателство не се преглежда непрекъснато;
- Използване на нелицензиран и неподходящ софтуер.

Е. РИСК КАТЕГОРИЯ - ПРАВЕН РИСК

Правният риск е свързан с неспособността на инфраструктурните процеси, системи и ресурси да поддържат спазването на правните и регулаторни изисквания. Това включва правна защита на интелектуалната собственост и други нематериални активи, възможност да се водят съдебни дела и управление на договорните отношения.

Подкатегория – Конкуренция. Рискове:

- Липса на разбиране за индустрията и пазара, в които организацията оперира;
- Неспособност да се постигне съответствие със съответните анти-монополни и ценообразуващи регулации;
- Неспособност да се разберат и да се преследват ползите от анти-монополните закони и регулации.

Подкатегория - Управление на договори. Рискове:

- Неспазване на клаузи и условия по споразумения;
- Неподходящо ниво на правомощия за сключване на договори;
- Споразуменията не са съобразени с целите на организацията;
- Условията по договора не отговарят на нормативните изисквания;
- Не се осъществява мониторинг над спазването на споразуменията от страните по договора;
- Неподходящо/недостатъчно задълбочено предварително проучване на бъдещи партньори.

Подкатегория – Разследвания. Рискове:

- Криминални и съмнителни практики;
- Неспособност да бъдат внедрени контроли срещу измама;
- Неправилно извършване на независими вътрешни разследвания;
- Липса на запознатост с нормативните изисквания;
- Липса на координация между правна дирекция и другите организационни структури.

Подкатегория - Околна среда, здраве и безопасност. Рискове:

- Не са създадени процедури, касаещи сигурността и околната среда;
- Липсват политики и процедури, които да осигурят спазване на стандартите за безопасност;
- Липса на запознатост с нормативните изисквания.

Подкатегория - Интелектуална собственост. Рискове:

- Не са регистрирани права на интелектуалната собственост;
- Не е гарантирана сигурността на чувствителна информация, свързана с интелектуалната собственост;
- Нарушение на правата;
- Неспособност да се гарантира употребата на интелектуалната собственост;
- Неспазване на международната нормативна уредба.

Подкатегория - Трудови отношения. Рискове:

- Трудовото законодателство не е залегнало в политиките за управление на човешки ресурси;
- Не се осъществява мониторинг на трудовото законодателство;
- Липса на запознатост на персонала относно трудовото законодателство.

Подкатегория - Спазване на нормативната и законовата уредба. Рискове:

- Неправилна комуникация на задължителни нормативни изисквания;
- Неспазване на нормативните изисквания;
- Липса на надзор;

- Не е установена и поддържана ефективна програма, осигуряваща съответствието.

Подкатегория - Закони за защита и конфиденциалност на данните. Рискове:

- Не са установени формални политики и програми за конфиденциалност и защита;
- Неспособност да се осъществят програмите по конфиденциалност на данните;
- Неспазване на приложимото законодателство.

Подкатегория - Записи и управление на информацията. Рискове:

- Не е установена политика за поддържане и съхранение на записи;
- Неспособност да се възпроизвеждат записи;
- Неспазване на законите и задълженията свързани със съхранение и поддръжка на записи;
- Липса на политика за запазване на документи;
- Липса на отговорност за надзора на задължително запазване и съхранение на документация.

IV. РИСК КЛАС / КАТЕГОРИЯ - СЪОТВЕТСТВИЕ

Целите на организацията, свързани с осигуряване на съответствие се отнасят до спазването на приложимите закони, регулации и стандарти и всички приложими външни и вътрешни политики и правила. Изисквания за съответствие са свързани с пазар, ценообразуване, данъци, околна среда, социално осигуряване на служителите, международна търговия и т.н. Приложимите закони и регулации установяват минимални стандарти на поведение, които организацията интегрира в целите за осигуряване на съответствие. Историята на съответствието (и съответно на несъответствието) на организацията може значително да повлияе положително (или отрицателно) на нейната репутация в обществото и на пазара.

Подкатегория - Комуникации и обучение. Рискове:

- Неподходящо комуникиране на въпроси, свързани със съответствието;
- Липса на програма за обучение, обхващаща цялата организация;
- Не са идентифицирани конкретни/специфични дейности, за които са приложими нови закони, регулации и политики;
- Неспособност да се проследи и осигури свидетелство, че е преминато задължително обучение.

Подкатегория - Култура на съответствието. Рискове:

- Неспособност да се създаде култура, в която въпросите, свързани със съответствието са третирани обективно и с необходимото внимание ;
- Неспособност да се осигурят подходящи инструменти и ресурси на персонала, с които да се постигне непрекъснато съответствие;
- Културата на съответствието не отговаря на стратегията на организацията;
- Не са установени програми за осигуряване на съответствието и не се предприемат дисциплинарни мерки.

Подкатегория - Управление на информацията относно съответствието. Рискове:

- Не са установени ефективни начини за управление на информацията;
- Проблеми и дейности, свързани със съответствието не се обсъждат редовно от ръководството;
- Липса на интегритет на информацията, която се използва за вземане на решения и управление на съответствието.

Подкатегория – Организация. Рискове:

- Не са определени изрично представители на ръководството, които отговарят за съответствието;
- Неподходящо разпределение на ресурси;

- Липса на авторитет и независимост.

Подкатегория – Докладване. Рискове:

- Не са идентифицирани и докладвани основни тенденции, свързани със съответствието;
- Неподходящи или недостатъчни ресурси за ефективното докладване на проблеми;
- Неподходящо докладване на значителни проблеми на външни заинтересовани лица.

Подкатегория - Контрол и мониторинг. Рискове:

- Не са установени превантивни и отчитащи контроли;
- Не са установени програми за мониторинг и тестване;
- Неспособност да се поддържат подобрения в контролите.

Подкатегория - Политики и процедури. Рискове:

- Не са създадени подходящи политики и процедури;
- Прекомерни или хаотични, противоречащи си политики и процедури;
- Не е установена отчетност и инструменти за измерване.

Подкатегория - Оценка на риска. Рискове:

- Неспособност да се идентифицират съществени рискове;
- Не са установени необходимите контроли, които да ограничат идентифицираните рискове;
- Неспособност да се комуникират рисковете на всички нива и във всички звена в организацията.

Подкатегория – Надзор. Рискове:

- Не е установена отчетност, отговорност и инструменти за измерване;
- Не е установен и поддържан надзорен контрол;
- Неспособност да се направи връзка между представянето по отношение на съответствието с управлението на представянето;
- Възнаграждението не е обвързано с персоналната отговорност.

V. РИСК КЛАС / РИСК КАТЕГОРИЯ – ДОКЛАДВАНЕ

Докладване: обобщаване, изготвяне, представяне и разпространение на финансова и нефинансова информация до заинтересованите лица на организацията. Докладването включва, както вътрешни отчети за ползване от ръководството, така и външни отчети, изисквани от местните закони и регулаторните органи. Рисковете в този клас са свързани с:

- Неадекватни, неподходящи или подвеждащи база данни, анализ и представяне, а също и оперативните процеси, използвани за подготвянето на финансовите отчети;
- Невъзможност за събиране на уместна и надеждна външна и вътрешна информация;
- Липсващо, неправилно или недостатъчно представяне на финансова информация до подходящите хора и др.

Подкатегория риск - Спазване на счетоводните стандарти. Рискове:

- Неспособност да се следят и спазват стандартите;
- Неспособност да се имплементират Международни стандарти за финансово отчитане.

Подкатегория риск - Финансово оповестяване. Рискове:

- Не се оповестява информация съгласно регулаторните стандарти;
- Неподходящо обсъждане и анализ от страна на ръководството.

Подкатегория риск - Наличие на финансова информация. Рискове:

- Липсва финансова информация, необходима за вземането на решения;
- Неспазване на приложимото законодателство и нормативни изисквания;
- Липса на интегритет и качество на данните.

Подкатегория риск - Невярна информация във финансовите отчети. Рискове:

- Лошо управление и надзор;
- Неспособност да бъде установена програма за етичност и съответствие;
- Липса на ефективен вътрешен контрол;
- Липса на разделение на отговорностите.

Подкатегория риск - Управленско докладване. Рискове:

- Недостатъчен обмен на информация;
- Не се докладват основни показатели;
- Неефективно представяне на информацията.

Подкатегория риск - Регулаторно докладване. Рискове:

- Неправилно докладване;
- Съществени грешки във финансовите отчети;
- Неспособност да се докладва относно ефективността на вътрешния контрол;
- Неправилна/погрешна оценка;
- Липса на вътрешен контрол над процесите по финансово докладване и интегрирането им с други процеси, основни дейности и дейности, насочени към съответствието;
- Неспособност да се идентифицират и коригират съществени слабости и недостатъци.

Подкатегория риск - Качество на отчетите. Рискове:

- Неспособност да се представи точна и пълна информация;
- Информацията не се представя навреме;
- Използват се остарели инструменти за докладване и информация.

Подкатегория риск - Законово-изисквани отчети. Рискове:

- Липса на осведоменост относно изискванията;
- Неспособност да се осигури точност на отчетите;
- Неподходящ или неправилен формат на представяне на информацията.

Подкатегория риск - Устойчиво докладване. Рискове:

- Неспособност да се оповести несъответствието със съответните закони и регулации свързани с околната среда;
- Неспособност да се представи устойчивостта като потенциална инвестиционна идея.

Подкатегория риск - Данъчно докладване. Рискове:

- Неадекватно данъчно третиране на финансовите данни;
- Несъответствие с изискванията;
- Неспособност да се представят данъчно основани баланси;
- Неадекватна глобална оценка на данъчните разпоредби.

Риск - регистър

						Присъщ риск										Остатъчен риск															
						Изключително голямо (9)										Почти сигурно (9)				Трябва да направим много повече (9)											
						Съществено (7)										Вероятно (7)				Трябва да направим повече (7)											
						Умерено (5)										Възможно (5)				Усилията, които полагаме за този риск, са напълно адекватни (5)											
						Малко (3)										Рядко (3)				Трябва да правим по-малко (3)											
						Несъществено (1)										Не е вероятно (1)				Трябва да правим много по-малко (1)											
Клас	Категория	Под-категория	Risk ID	Риск	Описание на риска	Оценка на влияние						Ср. Аритм. Оценка Влияние (I)	Оценка на вероятност						Ср. Аритм. Оценка Вероятност (P)	Стойност на риска (I+P)/2	КОНТРОЛ	Оценка на ефективност на контрола						Ср. Аритм. Оценка на ефективността на контрола (C)	Оценка на риска	Рейтинг	
						a	b	c	d	e	f		a	b	c	d	e	f				a	b	c	d	e	f				
УПРАВЛЕНИЕ И НАДЗОР /УН/	Корпоративно управление и надзор		УН								0						0	0							0	0					
УПРАВЛЕНИЕ И НАДЗОР /УН/	Етика		УН								0						0	0							0	0					
СТРАТЕГИЯ И ПЛАНИРАНЕ /СП/	Социална отговорност и устойчивост		СП								0						0	0							0	0					
СТРАТЕГИЯ И ПЛАНИРАНЕ /СП/	Външни фактори		СП								0						0	0							0	0					
СТРАТЕГИЯ И ПЛАНИРАНЕ /СП/	Планиране		СП								0						0	0							0	0					
СТРАТЕГИЯ И ПЛАНИРАНЕ /СП/	Стратегия		СП								0						0	0							0	0					
ОПЕРАТИВНА ДЕЙНОСТ И ИНФРАСТРУКТУРА /ОДИ/	Управление на активите		ОДИ								0						0	0							0	0					
ОПЕРАТИВНА ДЕЙНОСТ И ИНФРАСТРУКТУРА /ОДИ/	Финанси		ОДИ								0						0	0							0	0					
ОПЕРАТИВНА ДЕЙНОСТ И ИНФРАСТРУКТУРА /ОДИ/	Човешки ресурси		ОДИ								0						0	0							0	0					
ОПЕРАТИВНА ДЕЙНОСТ И ИНФРАСТРУКТУРА /ОДИ/	Информационни технологии		ОДИ								0						0	0							0	0					
ОПЕРАТИВНА ДЕЙНОСТ И ИНФРАСТРУКТУРА /ОДИ/	Правен		ОДИ								0						0	0							0	0					
СЪОТВЕТСТВИЕ /С/	Съответствие		С								0						0	0							0	0					
ДОКЛАДВАНЕ /Д/	Докладване		Д								0						0	0							0	0					

ПРИМЕРНИ КРИТЕРИИ ЗА ОЦЕНКА НА ВЛИЯНИЕТО

Влияние	Финанси	Репутация	Юридически / регулаторен	Фондове от ЕС	Цели на организацията		Служители	Дейности	Активи
Показатели за оценка на представянето / риска	Бюджет	Отразяване в медиите, обществени настроения, проверки	Брой съдебни искове, административно-наказателни санкции и др.	Получаване и използване	Стратегически цели	Оперативни цели	Здраве, физическа сигурност и текучество	Процеси/системи	Сигурност и собственост, разходи за ремонт
Изключително голямо	над 5% от бюджета	-Сериозни обществени прояви (протести, неподчинение), продължително обществено недоверие / накрънено обществено доверие -Външни проверки и разследвания (от различни контролни органи, в т.ч. органи на ЕС)	-Съдебни дела -Дейността е прекъсната поради промяна в нормативната уредба, като последица от влезли в сила съдебни или административни актове или договори	Фондовете от ЕС следва да бъдат върнати или са преустановени	Сбъдването на риска значително ще попречи на постигането на повече от една от стратегическите цели на организацията		-Смърт/живото-застрашаващи наранявания значителен брой представители на ръководството напускат организацията -Глобална пандемия	-Основните дейности са спрени -Неизправност на критично важни системи	-Загуба на съществено важни за дейността активи
Съществено	2-5% от бюджета	-Широко и/или негативно отражение в медиите на национално ниво (ТВ, печатни издания) -Регулярни обществени прояви (протести, неподчинение), накрънено обществено доверие	-Промяна в нормативната уредба, промяна в резултат на влезли в сила съдебни или административни актове и договорни отношения -Заплаха от големи глоби и други наказания	Фондовете от ЕС са замразени	Сбъдването на риска значително ще попречи на постигането на повече от една от оперативните цели на организацията		-Хоспитализация -Значителен брой служители напускат организацията	-Нормалните дейности са значително повлияни -Дейностите не съответстват на целите -Необходими са значителни усилия за корективни дейности	-Загуба на активи -Сериозни щети
Умерено	1% - 2% от бюджета	-Отражение в медиите, по-скоро неутрално, отколкото негативно -Спад в нивото на обществено одобрение, спад в доверието от страна на определени обществени групи -Проверка / разследване от страна на орган/Комитет в рамките на организацията	-Могат да бъдат наложени глоби или друго наказание -Някои неосновни дейности биха могли да бъдат спрени или променени поради правна намеса	Усвояването на фондовете от ЕС е неефективно или забавено	Сбъдването на риска ще има известни негативни последици за постигането на целите на организацията		-Сериозни наранявания (хоспитализация) -Сериозно медицинско лечение -Ограничен брой служители/представители на ръководството от определени функции напускат организацията	-Някои основни дейности трябва да бъдат реорганизирани -Някои функционалности на системата временно са в неизправност -Нормалните дейности са донякъде повлияни, временно може да има спад в качеството -Някои изисквания не се спазват	-Частични щети са причинени на активите, които изискват ремонтни работи или замяна
Несъществено	до 1% от бюджета	-Ограничено отражение в медиите -Индивидуалния/институционния рейтинг може да спадне; -Отрицателната реакция е от страна само на ограничена група хора -Вътрешен преглед (в рамките на Дирекцията)	-Няма заплаха от съдебни искове -Минимални глоби	Ограничен ефект над фондовете от ЕС	Сбъдването на риска ще им малко влияние над постигането на оперативните цели на организацията;		-Леки наранявания, изискващи първа помощ / не изискващи медицинско лечение -Ограничени последици за текучеството на персонала	-Незначителни грешки в системата или процесите, които могат да бъдат отстранени с корективни дейности	-Ефектът над активите е изисква минимални ремонтни работи
Малко	до 0.5% от бюджета	-По-скоро неутрално/никакво отражение в медиите -Индивидуалния/институционния рейтинг може да спадне за много кратък период -Само определни служители са обект на проверка	-Няма последици	Никакъв ефект над фондовете от ЕС	Сбъдването на риска няма да окаже влияние над постигането на целите, но може да зстраши изпълнението на определени задачи		-Никакви последици за текучеството на персонала	-Някои дейности са забавени, но с незначителен/никакъв ефект над качеството	-Ефектът над активите е сравним с нормална амортизация

Приложение 4

ПРИМЕРЕН ПЛАН ЗА ДЕЙСТВИЕ

Цел 1	Риск	Действия/Мерки	Отговорен служител	Отчет на... за (дата/резултат)	Краен/ междинен срок за изпълнение

ПРИМЕРЕН КАЛЕНДАР НА ЗАСЕДАНИЯТА НА КОМИТЕТА ПО РИСКА

Януари Поставяне на целите на звената Идентифициране и оценка на риска	Февруари Изготвяне на План за действие	Март Месечна среща в рамките на дирекцията (при необходимост)	Април Месечна среща в рамките на дирекцията (при необходимост/
Май Месечна среща в рамките на дирекцията (при необходимост)	Юни Полугодишно заседание на Комитета по риска за обсъждане на необходимостта от актуализиране на оценката на риска и Плана за действие шестмесечна среща в рамките на дирекцията (задължителна)	Юли Месечна среща в рамките на дирекцията (при необходимост)	Август Месечна среща в рамките на дирекцията (при необходимост)

Приложение 6

Септември	Октомври	Ноември	Декември
Месечна среща в рамките на дирекцията	Месечна среща в рамките на дирекцията (при необходимост)	Месечна среща в рамките на дирекцията (при необходимост)	Годишно заседание на Комитета по риска за отчитане на резултатите и изготвяне на доклад за УР до Директора

Приложение 7

РЕГИСТЪР НА ПРОЯВИЛИ СЕ РИСКОВЕ

[illegible]



**БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО ФИЗИОЛОГИЯ НА РАСТЕНИЯТА И ГЕНЕТИКА**

ул. "Акад. Г. Бончев", бл. 21, 1113 София

Директор: 02/979-26-06; Зам. директор: 02/979-26-20

Ел. поща: office-ifrg@bio21.bas.bg; ifrg@bio21.bas.bg

Интернет: <http://www.bio21.bas.bg/ippg/>

ЗАПОВЕД

На основание чл. 25, ал. 4, т. 5 от Устава на БАН и във връзка с чл. 12, ал. 3 от Закона за финансовото управление и контрол в публичния сектор (ЗФУКПС)

УТВЪРЖДАВАМ

Стратегия за Управление на риска в Българска академия на науките, с период на действие 2023-2025 година.

Настоящата заповед да се доведе до знанието на всички служители в ИФРГ-БАН за сведение и изпълнение.

Директор:

(проф. д-р Валя Василева)