DELIVERABLE 4.4.3 Implementation of boosting business skills short sessions

TRAINING MATERIAL FOR EXISTING ENTREPRENEURS ON TOPIC:

“RISK ANALYSIS AND RISK MANAGEMENT”

Beneficiary’s Name:

LOCAL ECONOMIC DEVELOPMENT AGENCY - RAZLOG (BULGARIA)

The Project is co-funded by the European Regional Development Fund (ERDF) and by national funds of the countries participating in the Interreg V-A “Greece-Bulgaria 2014-2020” Cooperation Programme

Contract No. B6.3a.28/26.04.2021 for the project "Empowering businesses Seeking Growth",/SeeG under priority axis 1: Competitive and innovative cross-border region, investment priority 3a - Encouraging entrepreneurship, in particular by facilitating the economic use of new ideas and encouraging the creation of new companies, including through business incubators of the Cross-Border Cooperation Program INTERREG V-A "Greece-Bulgaria" 2014-2020

Training material

for active entrepreneurs and existing businesses

RISK ANALYSIS AND RISK MANAGEMENT

The Project is co-funded by the European Regional Development Fund (ERDF) and by national funds of the countries participating in the Interreg V-A "Greece-Bulgaria 2014-2020" Cooperation Programme

SUMMARY

The training material "Risk analysis and risk management" was prepared during the implementation of the activity "Development of training materials and translations of content for an electronic platform within the project "Empowering businesses Seeking Growth" with the acronym SeeG, financed under a grant contract aid B6.3a.28 / 26.04.2021 under priority axis 1: Competitive and innovative cross-border region, investment priority 3a - Encouraging entrepreneurship, in particular by facilitating the economic use of new ideas and encouraging the creation of new companies, including through business incubators of the Cross-Border Cooperation Program INTERREG V-A "Greece-Bulgaria" 2014-2020.

The training material will help you understand how to analyze and manage risks. For this purpose, the terms "risk", "risk identification", "risk analysis", "risk management", "risk management process" and "risk management system", as well as the applicable standards, will be introduced and explained. Examples, practical guidelines and guidelines that can be used by entrepreneurs are presented.

Risk management is a part of business management that deals with the assessment and management of risks for an enterprise. It plays a major role in project management and other new ventures. It often finds a place in the drafting of business plans.

Formally, risk management is a process in which the development of existing risks is investigated, analyzed and tracked in order to reduce the negative effect of their eventual occurrence or to provide an opportunity to benefit from their occurrence.

Risk management aims to be proactive – dealing with harms / opportunities long before they become a reality.

An organization's risk management process consists of eight interrelated elements:
Determination of the internal environment;
 Formulation of goals;
 Identification of risks;
 Risk assessment;
 Responding to risk;
 Determination of means of control;
Creating conditions for receiving, processing and transmitting information. Defining the terms of communication;
 Monitoring.
Risk management is thus defined as a process. It emphasizes the mutual relationship between the goals of the organization (strategic, operational, tasks, compliance with the regulations), the organizational structure of the company (levels of the organization, subdivisions, business units and others) and the other elements of risk management.
Risk management is considered as a part of the strategic management of the organization, the task of which is the identification of risks and their management, and the system also includes a

program to control the implementation of the assigned tasks, evaluation of the effectiveness of the activities carried out and a system for encouraging all levels of the organization.

The Federation of European Risk Managers' Associations (FERMA) Risk Management Standard 2003 is a joint development with several leading UK risk management organisations: Institute of Risk Managers (IRM), The Risk Association -management and insurance (AIRMIC), the National Forum for Risk Management in the Public Sector (ALARM).
The standard defines four groups of risks:

- ✓ strategic,
- ✓ operational,
- ✓ financial risks
- ✓ dangers.

The key stages of the risk management process are characterized.

Risk management issues are addressed in international standards relating to various areas of human activity – for example, occupational safety and health, food safety, information security, environmental management and others. It has been reported that there is a need for the creation of a unified risk management technology to be used in organizations from all spheres of society, including the intangible.
In 2009, the International Organization for Standardization issued ISO 31000:2009 Risk Management – Principles and guidelines on implementation and ISO 31010:2009 Risk Management – Risk assessment guidelines Risk Assessment).

The above international standards are not intended for individual spheres or fields of activity. They can be used by any type of organization – government, private, non-governmental and others. In addition, the standards can be applied to the management of different types of risks, are not mandatory and do not require certification. Therefore, the standards offer a common approach to specific risks and at the same time guide organizations to develop their own risk management approaches.
The risk management system can ensure the fulfillment of a number of management objectives of the organization. It can be the basis of all management activity and can serve as the basis of the management strategy and the control system.

Договор № B6.3a.28/26.04.2021 за проект „Овластяване на бизнеса, търсещ растеж“Empowering businesses Seeking Growth,/SeeG по приоритетна ос 1: Конкурентен и иновативен трансграничен регион, инвестиционен приоритет 3a - Насърчаване на предприемачеството, по-специално чрез улесняване на икономическото използване на нови идеи и насърчаване на създаването на нови фирми, включително чрез бизнес инкубатори на Програмата за трансгранично сътрудничество INTERREG V-A „Гърция-България” 2014-2020

Обучителен материал

за действащи предприемачи и съществуващи предприятия

РИСК АНАЛИЗ И УПРАВЛЕНИЕ НА РИСКА

The Project is co-funded by the European Regional Development Fund (ERDF) and by national funds of the countries participating in the Interreg V-A “Greece-Bulgaria 2014-2020” Cooperation Programme

РЕЗЮМЕ

Обучителният материал „Риск анализ и управление на риска” е изготвен при изпълнение на дейност „Разработване на обучителни материали и преводи на съдържание за електронна платформа в рамките на проект „Empowering businesses Seeking Growth” с акроним SeeG, финансиран по договор за предоставяне на безвъзмездна финансова помощ B6.3a.28 / 26.04.2021 г. по приоритетна ос 1: Конкурентен и иновативен трансграничен регион, инвестиционен приоритет 3а - Насърчаване на предприемачеството, по-специално чрез улесняване на икономическото използване на нови идеи и насърчаване на създаването на нови фирми, включително чрез бизнес инкубатори на Програмата за трансгранично сътрудничество INTERREG V-A „Гърция-България” 2014-2020.

Обучителнинят материал ще Ви помогне да разберете как да анализирате и управлявате рисковете. За целта ще бъдат въведени и обяснени термините „риск”, „идентифициране на рискове”, „риск-анализ” „управление на риска”, „процес за управление на риска” и „система за управление на риска”, както и приложимите стандарти. Представени са примери, практически указания и насоки, които могат да бъдат изполлзвани от предприемачите.

Управление на риска е дял от стопанското управление, който се занимава с оценка и управление на рисковете за едно предприятие. То играе основна роля при управлението на проекти и други нови начинания. Често намира място и при съставянето на бизнес планове.
Формално, управлението на риска е процес, при който се изследва, анализира и проследява развитието на съществуващите рискове с цел да се намали негативния ефект от евентуалното им настъпване или да се предостави възможност за възползване от тяхното настъпване.
Управлението на риска има за цел да бъде проактивен – да работи с вредите / възможностите много преди те да станат реалност.

Процесът на управление на рисковете на организацията се състои от осем взаимносвързани елемента:

- Определяне на вътрешната среда;
- Формулиране на целите;
- Идентифициране на рисковете;
- Оценка на риска;
- Реагиране на риска;
- Определяне на средствата за контрол;
- Създаване на условия за получаване, обработване и предаване на информацията. Определяне условията за комуникация;
- Мониторинг.

По този начин **управлението на риска се определя като процес**. В него се акцентира на взаимната връзка между целите на организацията (стратегически, оперативни, задачи, спазването на нормативната уредба), организационната структура на фирмата (равнища на организацията, подразделения, стопански единици и други) и останалите елементи на управлението на риска.

Управлението на риска се разглежда като част от стратегическото управление на организацията, чиято задача е идентифицирането на рисковете и тяхното управление, като в системата се включва и програма за контрол на изпълнението на поставените задачи, оценка на ефективността на провежданите мероприятия и система за поощряване на всички равнища на организацията.

Стандартът за управление на рисковете на Федерацията на европейските асоциации на риск-мениджърите 2003 (FERMA) е съвместна разработка с няколко водещи организации от Великобритания, които се занимават с въпросите на управлението на риска: Институт на риск- мениджърите (IRM), Асоциацията за риск-мениджмънт и застраховане (AIRMIC), Националния форум за риск-мениджмънт в обществения сектор (ALARM).
Стандартът определя четири групи рискове:

- ✓ стратегически,
- ✓ оперативни,
- ✓ финансови рискове
- ✓ опасности.

Характеризирани са ключовите стадии на процеса на управление на риска.

Въпросите за управлението на риска са третирани в международни стандарти, отнасящи се до различни области на човешката дейност – например, безопасността и здравето при работа, безопасността на храните, сигурността на информацията, управлението на околната среда и други. Отчетено е, че се появява необходимост от създаването на единна технология за управлението на риска, която да бъде използвана в организациите от всички сфери в обществото, вкл. нематериалната.
През 2009 г. Международната организация по стандартизация издава ISO 31000:2009 Risk Management – Principles and guidelines on implementation (Риск-мениджмънт – Принципи и ръководство за прилагане) и ISO 31010:2009 Risk Management – Risk assessment guidelines (Риск-мениджмънт –Ръководство по оценка на риска).

Горепосочените международни стандарти не са предназначени за отделни сфери или области на дейност. Те могат да бъдат използвани от всякакъв вид организации – държавни, частни, неправителствени и други. Освен това стандартите могат да бъдат прилагани към управлението на различни видове рискове, не са задължителни и не се изисква по тях да бъде извършвана сертификация. Следователно, стандартите предлагат един общ подход към специфични рискове и същевременно насочват организациите към разработването на свои подходи за управление на рисковете.

Системата за управление на риска може да осигури изпълнението на редица управленски цели на организацията. Тя може да бъде в качеството си на основа на цялата управленска дейност и може да служи за основа на управленската стратегия и системата за контрол.

ВЪВЕДЕНИЕ

Проект **SeeG** "Empowering businesses Seeking Growth" *(в превод на български език „Овластяване на бизнеса, търсещ растеж")* има за цел да стимулира и повиши устойчивото предприемачество чрез трансгранично сътрудничество, допринасяйки за икономическото развитие на региона; да създаде екосистема, подкрепяща предприемачите, чрез приспособяване на услуги за техните реални нужди; да подкрепи приоритетни и основни предприемачески услуги в географски райони с относителна липса на системи за подкрепа.

Предприемат се серия от дейности и инициативи за справяне с пречките, които ограничават малките и средни предприятия (МСП) и се осигурява достъп и подкрепа до съществуващи услуги. Трансграничната област, както е посочено в неотдавнашните проучвания на RIS3, показва много лоши резултати в иновативното предприемачество, а връзките между академичната общност и бизнеса са много слаби. Двете страни имат общи нужди за свързване на академични изследвания с бизнеса, за обединяване на предприятията с цел преодоляване на недостатъците, създаване на мрежи и укрепване на мобилизацията.

За да се подобрят системите за подпомагане на предприемачеството в МСП, се предвижда набор от дейности, чрез разглеждане на два основни вида фактори – определяне вземането на решения за нови бизнеси и определяне успеха и жизнеспособността на предприятията.

В първия случай дейностите са от значение за повишаване на знанията; генериране на бизнес идеи; способности за достъп до финансиращи инструменти; възможности за работа в мрежи и развитие на умения, свързани с въпроси като управление на риска и т.н.

Във втория случай дейностите са насочени към предприемачески аспекти като квалифицирани ресурси, качествени и иновационни инструменти, техники за въвеждане на процедури, маркетинг и популяризиране на бизнес стратегии и т.н.

Проектът цели повишаване културата на предприемачеството, подпомагане създаването на бизнес, изграждане на нови умения и подкрепа на нови и/или съществуващи предприятия.

Този материал е изготвен при изпълнение на дейност „Разработване на обучителни материали и преводи на съдържание за електронна платформа в рамките на проект „Empowering businesses Seeking Growth" с акроним SeeG, финансиран по договор за предоставяне на безвъзмездна финансова помощ B6.3a.28 / 26.04.2021 г. по приоритетна ос 1: Конкурентен и иновативен трансграничен регион, инвестиционен приоритет 3а - Насърчаване на предприемачеството, по-специално чрез улесняване на икономическото използване на нови идеи и насърчаване на създаването на нови фирми, включително чрез бизнес инкубатори на Програмата за трансгранично сътрудничество INTERREG V-A „Гърция-България" 2014-2020.

РИСК – АНАЛИЗ И УПРАВЛЕНИЕ НА РИСКА

Обучителен материал за съществуващи предприемачи/предприятия

I. СЪЩНОСТ НА РИСКА В ИКОНОМИЧЕСКИ АСПЕКТ

1. Термини, произход и определения.

- **РИСК**

Рискът се отнася до отклонението от един или повече резултати на едно или повече бъдещи събития от тяхната очаквана стойност. Технически, стойността на тези резултати може да е позитивна или негативна. Положителния риск се разглежда като *възможност*, а при общата употреба на думата *риск* се фокусира само върху потенциалната вреда (загуба на позитивни резултати), която може да възникне от бъдещо събитие, което да произтече или от влизане в разноски ("риск от снижение" - на английски: *downside risk*) или от неспособност да се придобие някаква печалба ("риск на изкачването" – на английси: *upside risk*).

Думата *риск* произлиза от среднофренската *risque*, която е от италианската *risco* (в съвременния италиански вече е *rischio*), свързана с глагола *rischiare* – „натъквам се, попадам на опасност“, „бивам застрашен“. Допуска се, че тези италиански думи имат латински произход и са свързани с латинската *resicum* – „това, което реже, разбива“ (забележи близостта с българската *режа*), която е от средновековно латинската *resicu* и *resecō* – „отрязвам“, „отвързвам“ в смисъл на „давам началото на нещо лошо“) или древногръцки произход: от *ῥιζικόν*. Има предположения и за семитски произход.

- **УПРАВЛЕНИЕ НА РИСКА**

Управление на риска е дял от стопанското управление, който се занимава с оценка и управление на рисковете за едно предприятие. То играе основна роля при управлението на проекти и други нови начинания. Често намира място и при съставянето на бизнес планове.

Формално, **управлението на риска е процес, при който се изследва, анализира и проследява развитието на съществуващите рискове с цел да се намали негативния ефект от евентуалното им настъпване или да се предостави възможност за възползване от тяхното настъпване.** Управлението на риска има за цел да бъде проактивен – да работи с вредите / възможностите много преди те да станат реалност.

Голяма част от рисковете, които могат да сполетят едно начинание е възможно да бъдат предвидени. Те се наричат *известни рискове*. Това са и тези рискове, които могат да бъдат управлявани. Остава и части, които няма как да бъдат предвидени. Такива рискове се наричат *неизвестни*. Такива рискове могат да бъдат контролирани само с техники като предвиждане на финансов, времеви или материален резерв.

Управлението е процес, който предполага изпълнението на поредица от операции :

- **първата е осъзнаване на проблема, който трябва да се реши;**
- **втората - подготвяне на решение, свързано преди всичко със събиране на информация**
- **трета - приемане на решението, което може да бъде отразено с различни актов, подпис на договори.**

Управление на риска само по себе си не съществува, никой не рискува заради самия риск. Риска е характеристика на управлението на някаква конкретна дейност от тази гледна точка е некоректно да се изисква словосъчетание управляване на риска. Анализа и контрола на риска е процес, който е институционално закрепен, има наредби които регламентират този процес и той се нарича оценка на риска. Анализа и контрола са два препокриващи се частично процеса всеки от които включва относително особени процедури:

1. Разкриване на риска - свързва се с анализа и класификацията на риска на опасностите на фактите и причините за тяхното появяване и трансформиране от абстрактни в реални.
2. Оценка на риска - свързва се с количествения анализ с оглед установяване вероятността, да се случи нежелано събитие или тежестта на вредата, размера на щетите, които може да причини.

За оценяване на риска има няколко различни метода. Най- ефективния е този, който се основава на статистическите данни, той се използва в застрахователното дело, кредитирането и др. Недостатък при него е, че се използва само за еднородни,често повтарящи се събития. За оценка на други уникални събития се използват други методи, например метода с проследяване на последователността от възможни инциденти. Тези инциденти могат да бъдат от различно естество, като отказ на някой определен елемент от системата, неправилно използване на оборудването, не използване на необходимата предпазна техника и т.н..Причините за настъпване на нежелано събитие могат да бъдат различни в случая важното е да се покаже същността на този метод, който трябва да изчисли вероятността на всеки един такъв отказ или не изпълнението на задълженията и на тази основа да се изчисли вероятността да не се постигне крайната цел.При този метод могат да се използват графични средства, като се тръгна от първичния инцидент и като се проследи какви могат да последиците за системата в зависимост от това дали ще заработва ефективни предпазни мерки. Стига се до поставяне на дърво на отказите, но е необходимо да се изгради графичен модел, всички инциденти и всички откази да бъдат описани. Например какво ще стане, ако е изхабена спирачната течност.

Друг метод е този, който анализира в обратна посока от последиците- инцидент- събития - проследяване на пътищата довели до него - дърво на отказите, т.е всяка причина е клон, всяко разклонение е причина довела до нежелателни последици.

При оценяването възникват и проблеми. Тази оценка и съпоставяне с финансови и икономически състояния на този който взема решението имат важен аспект, имуществените щети се изчисляват в материален аспект. Чрез определени методи щетите могат да придобият парична форма, тогава се говори за защити. Но не винаги придобитата парична форма покрива в реални размери щетите.

- **ИДЕНТИФИЦИРАНЕ**

Идентифицирането на рискове е процес, при който се определят възможните източници на рискове, а самите рискове се идентифицират и описват.

Източниците на рискове в контекста на конкретен проект могат да бъдат разделени в две основни групи: външни и вътрешни. *Външните рискове* обикновено произлизат от бизнес средата, в която функционират участниците в проекта (имат икономически, социален, политически или технологически характер), от висшия мениджмънт (пр. промяна в собствеността на организацията, промяна в бизнес целите и стратегиите, вътрешна нестабилност и конфликти и т.н.) и от клиентите на проекта (пр. липса на заинтересованост и ангажираност, организационно културни различия т.н.). Наричат се външни, защото проектния екип (в това число и проектния мениджмънт) не може пряко да им влияе. Идентифицирането на външните рискове е най-успешно при наличието на задълбочен анализ на външната (макросреда и микросреда) и вътрешната среда (висш мениджмънт, финансови/човешки ресурси и т.н.) на ниво организация. *Вътрешните рискове* са свързани със самия проект и типа задачи, които се изпълняват в него. Тези рискове са малко или много под контрола на проектния екип (проектния мениджър) и с възрастта на организацията и натрупването на опит, значително намалява. Например такива рискове могат да са резултат от неяснота в ролите и отговорностите вътре в екипа, липсата на дисциплина и ред, липсата на управленски качества и познания, липсата на мотивация (риск от текучество), внедряването на нова технология и т.н. Също така трябва да се прави разлика между *общи рискове* (присъщи за всички проекти) и *специфични рискове*;

- **АНАЛИЗ И ОЦЕНКА**

Анализът и оценката на рисковете е процес, при който рисковете се анализират с цел да се определят вероятността те да се сбъднат и евентуалните последиците върху проекта. Целта е да се постави количествена оценка на всеки риск на база, на която те да бъдат приоритизирани (за целите на модифицирането им). Тук обаче трябва да се вземе предвид факта, че конкретния момент на настъпване на риска има значение върху последиците, които ще окаже. Използвайки тези два показателя се въвежда т.нар. матрица за оценка на степента на риска.

Оценката, която се получава като резултат от тези два показателя се нарича влияние на риска. Съществуват два подхода за оценяването на рисковете: отгоре-надолу и отдолу-нагоре. При подхода отгоре – надолу се разработва списък на потенциалните рискови фактори. Оценката е на база предишен опит. Стремежът е да се определят потенциалните връзки между отделните рискове, моментите на тяхното настъпване и възможните последици. Това дава възможност да се вземат предварителни действия за да се предотврати или намали влиянието на риска. При подхода отдолу – нагоре рисковете се анализират детайлно на най-ниското ниво. Оценяват се алтернативните критични пътища и се изчисляват времетраенето и продължителността с цел да се осигури възможност на ръководителите да заложат буфери, с помощта на които биха посрещнали негативните последици от реализирането на рискове. На практика този подход предполага невъзможност на ръководителя да предвиди риска и да предприеме превантивни управленски действия за избягването му.

- **РИСКЪТ ВЪВ ФИНАНСИТЕ**

Понятието *риск* има широка употреба във финансовите теория и практика. Различават се следните видове риск: кредитен, ликвиден, държавен (суверенен), пазарен (свързан с цените: риск на ценните книжа, лихвен, валутен, продуктов).

Има съществена разлика между видовете риск във финансите и финансовия риск. Финансовият риск е един от тези видове и той е свързан със степента на използване на заемни средства в капиталовата структура на едно предприятие, с други думи това е *финансовият ливъридж* или наричан още *финансов лост*.

Бизнес рискът описва дела на постоянните разходи в състава на общите разходи. Този риск се поема от акционерите.

- **ПОДХОДИ КЪМ РИСКА**

Отговорът спрямо даден риск може да бъде:

- Избягване – Понякога е възможно организацията да бъде променена така, че рискът да бъде избегнат;
- Трансфериране / споделяне – трансферирането е изнасяне на идентифицирания риск към външна организация. Типични примери за трансфериране са аутсорсинг или застраховане и хеджиране за случаи на финансови рискове;
- Омекотяване / ограничаване – ако рискът не може да бъде избегнат, приемлива алтернатива е да бъде омекотен чрез стъпки, които ще сведат до минимум щетите в случай на рисково събитие;
- Приемане – когато няма какво да се предприеме в отговор на риска, единствената възможност, която остава е той да бъде осъзнат и приет.

- **БИЗНЕС РИСК**

Бизнес рискът *(Business risk)* се определя като „риск, възникващ в резултат на важни условия, събития, обстоятелства, действия или бездействия, които биха могли да се отразят неблагоприятно върху способността на предприятието да постигне целите си и да изпълни стратегиите си, или риск, възникващ в резултат на неподходящо определени цели и стратегии“ (вж. МОС 315.4). Той е по-широкообхватен от РСНО във финансовите отчети и може да възникне в резултат на промени или сложност на операциите

Разбирането за бизнес рисковете е предпоставка за идентифициране на РСНО, тъй като повечето бизнес рискове имат финансови последици и следователно влияят върху финансовите отчети.

Бизнес риск може да породи РСНО за класове сделки и операции, салда по сметки и оповестявания на ниво твърдение за вярност или на ниво финансов отчет. Това обаче зависи от конкретните обстоятелства, свързани с предприятието. Например бизнес риск, който възниква вследствие на намаляваща клиентска база, може да повиши риска от съществени отклонения, свързани с оценката на вземанията (вж. МОС 315, пар. А41). Възможно е бизнес рисковете да действат в комбинация, което би имало дългосрочни последици за предприятието (например икономика в рецесия съчетано със загуба на клиенти).

Възможността бизнес риск да доведе до РСНО следва да се разглежда в светлината на свързаните с предприятието обстоятелства. В теорията и

практиката се предлагат различни класификации на бизнес рисковете в зависимост от конкретните фактори и обстоятелства, пораждащи възникването им. Най-общо те могат да се разделят на:

а) външни, които, от своя страна, могат да бъдат класифицирани като: социални, културни, политически, правни, финансови, технологични, икономически, стратегически, оперативни, природни, рискове от физическа опасност и др.; и

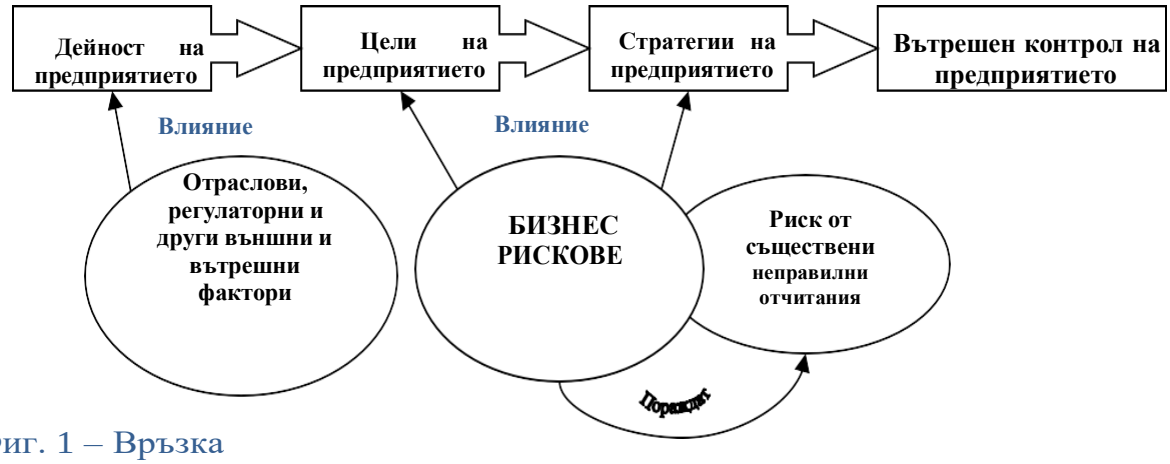
б) вътрешни, включващи: управлението, структурата, ресурсите (материални и човешки), ролите и отговорностите на организацията.

Процесът на предприятието за оценка на риска като компонент на вътрешния контрол. Бизнес рискове

Процесът на предприятието за оценка на риска (Entity's risk assessment process) най-общо представлява идентифициране, оценка и противодействие на бизнес рисковете чрез въвеждане на контролни дейности. Предприятието внедрява контроли, за да осигури разумна степен на сигурност, че ще постигне поставените цели. Тези цели и следователно контролите са свързани с финансовото отчитане, операциите и спазването на изискванията.

Върху целите и стратегиите на предприятието и тяхното постигане и изпълнение влияние оказват бизнес рисковете, които могат да породят риск от съществени неправилни отчитания (РСНО). Познаването на целите и стратегиите на предприятието и онези бизнес рискове, които могат да породят РСНО, ще осигури възможност за адекватна оценка на процеса на предприятието за оценка на риска.

Връзката между цели и стратегии и бизнес рисковете, пораждащи РСНО, е представена в следващата схема (фиг. 1):



Фиг. 1 – Връзка между цели, стратегии и бизнес рискове

- **ПРИМЕРИ ЗА БИЗНЕС РИСКОВЕ:**

В систематизиран вид възможни бизнес рискове и съответните контролни дейности са представени в следващата таблица (табл. 1)

№ по ред	Възможни бизнес рискове	План за действие, контролни дейности
1.	Глобални, регионални или национални здравни епидемии и пандемии	1. Използване на компенсационни механизми, предоставени от правителството (помощи, кредити и други стимули) 2. Застраховане срещу спад в приходите или спиране на производството 3. Пренасочване по възможност на ресурси в дейности, които създават нови възможности (например производство на защитни и предпазни средства, оборудване или храни) 4. Кооперирane на доставките и производството за намаляване на разходите 5. Пренасочване на персонала в дейности по поддръжка, ремонт и обновяване на сгради, машини и оборудване или други подобни дейности 6. Използване на отпуски (платени и неплатени) или подписване на споразумения за временно намаляване на заплатите с персонала в периода на епидемията
2.	Война, военни конфликти, терористични актове	1. Прехвърляне на част или цялата дейност в други райони, незасегнати от конфликта 2. Съхраняване на най-важните дълготрайни активи и материални запаси в сигурни складови помещения 3. Разработване на процедура за евакуация на служителите в случаите на непосредствена физическа заплаха 4. Процедура за докладване на инциденти 5. Застраховане

3.	Влошаване на общата икономическа и политическа обстановка в страната	1. Промяна на бизнес планове 2. Преразглеждане на стратегия за развитие 3. Актуализиране и преглед на плановете за непредвидени случаи 4. Диверсифициране на пазари, клиенти, доставчици 5. Планове за прехвърляне дейността в страни със стабилна политическа обстановка и икономика 6. Запазване на ключов персонал 7. Замразяване на инвестиции, изискващи много финансови средства за реализирането им или на инвестиции с по-висок риск
4.	Промени в приложимата обща рамка за финансово отчитане и приложимото законодателство	1. Обучение на счетоводния персонал 2. Консултации с одитор 3. Консултации с експерти 4. Актуализиране на счетоводния софтуер
5.	Спазване на закони, нормативни актове и правителствени политики, засягащи дейността на дружеството	1. Поддържане и използване на програмни продукти и книжни издания с актуалната нормативна база 2. Активно участие в публичните обсъждания по отношение планирани промени в нормативната уредба, касаеща дейността на дружеството 3. Използване на услугите на консултантски фирми 4. Редовни консултации и обсъждане на нови или променени нормативни изисквания с правния отдел на предприятието
6.	Грешна бизнес стратегия	1. Установяване на ясни цели и стратегии 2. Промяна на целите и стратегиите 3. Редовно преразглеждане на стратегията и актуализирането ѝ съгласно пазарните условия и промени
7.	Промени на валутните курсове	1. Предоговаряне на договорите във валути със стабилен валутен курс 2. Използване на бартерни сделки 3. Фиксиране на курса чрез сключване на предварителни договори за обмяна на валута 4. Застраховка срещу рискове от промяна във валутните курсове 5. Използване на специализирани FOREX продукти
8.	Увеличение на инфлацията	1. Промяна на складовите наличности на материални запаси 2. Търсене на алтернативни доставчици

9.	Значителни промени и развития в отрасъла (технологично и продуктово развитие)	1. Промяна и ускоряване на развойната дейност 2. Промени в плана за инвестиции 3. Сключване на договори с високо квалифициран персонал 4. Търсене на експертни решения от консултанти в отрасъла
10.	Засилване на конкуренцията в отрасъла	1. Промяна на маркетинговата стратегия 2. Търсене на нови клиенти 3. Актуализация на цените
11.	Разширяване на бизнеса	1. Промяна на оценките за търсенето 2. Промяна на маркетинговите планове 3. Контрол и преглед на бюджетите и инвестициите
12.	Честа промяна на цените на суровини и материали	1. Изготвяне на стратегия за групите суровини и материали, подложени на чести ценови промени 2. Мониторинг и проследяване на ценовите тенденции 3. Оптимизиране на запасите след извършване на анализ на ползите и разходите от увеличение (при очакван спад в цените) или намаление (при очаквано повишение на цените) на запасите от суровини и материали
13.	а) Некоректни клиенти – забавяне на плащания, неплащане, промяна на условия по договори б) Фалит и несъстоятелност на клиенти	1. Изваждане от списъка с одобрени клиенти 2. Преговори с клиентите и сключване на нови или допълнителни споразумения 3. Установяване на лимити по конкретни клиенти съгласно финансовата им история 4. Промяна на утвърдени срокове за плащане или увеличаване на авансовите плащания 5. Избягване на зависимостта от малко на брой клиенти с голям дял в продажбите и преход към по- голям брой клиенти с по-малък дял в продажбите 6. Периодичен мониторинг на вземанията и подобряване на аналитичната отчетност 7. Завеждане на съдебни дела 8. Използване на услугите на колекторски фирми 9. Сключване на договори за цесия
14.	Намаляване на удовлетворе-ността на клиентите	1. Идентифициране на източниците на проблема – трудно е да се прави бизнес с предприятието или продуктите (услугите) са с влошено качество 2. Използване на софтуер за управление на взаимоотношенията с клиентите 3. Преглед на качеството на продуктите (услугите) и увеличаване на контрола на качеството 4. Провеждане на анкети с клиентите 5. Обучение на персонала, зает с продажбите

15.	а) Некоректни доставчици – забавяне на доставки или промяна на условия по договори б) Фалит и несъстоятелност на доставчици	1. Изваждане от списъка с одобрени доставчици 2. Разширяване на кръга на одобрените доставчици 3. Подобряване на процедурите за проверка на финансовата история на доставчиците, включително разширяване на външните източници на информация за доставчиците 4. Завеждане на съдебни дела към доставчици по аванси
16.	Новите продукти не отговарят на очакванията на потребителите или съществуват продукти, трудни за продаване	1. Идентифициране на силни и слаби страни на продукта с цел подобрение. 2. Промяна в маркетинговия план и рекламата 3. Провеждане на допълнително обучение на персонала, зает с продажбите 4. Анализ на това дали се продава на правилния пазар и правилните клиенти
17.	Съдебни дела срещу предприятието	1. Намаляване на споровете по договори чрез използване на стандартни срокове и условия по договорите 2. Използване юридически консултации от съществуващ в предприятието правен отдел или от външни фирми 3. Съгласуване на договорите с правния отдел или външна правна кантора 4. Разширяване и подобряване на обучението на служители, ангажирани с изготвянето на договори 5. Застраховане срещу рискове от съдебни дела
18.	Промишлен и търговски шпионаж	1. Въвеждане на ефективна политика за сигурност – като забраняване на споделянето на пароли и носене на собствени устройства за записване на данни на работа 2. Поддържане на ефективна политика за достъп до данните 3. Защитаване на критичната ИТ инфраструктура – използване на пароли за достъп, антивирусни програми, програми за неутрализиране на зловреден софтуер, използване на криптирана връзка и протоколи за сигурност, криптиране на информацията 4. Съхраняване на ценна информация на хартиен носител в каси и сейфове с ограничен достъп 5. Обучение на персонала на основните практики за сигурност, които трябва да спазват в ежедневната си работа – като например заключване на екрана на компютъра, ако не се използва или е без надзор за определено време, използване на сигурни пароли 6. Проследяване на активността на служителите относно контактите им със съмнителни лица 7. Видеонаблюдение и преглед на кореспонденцията на работното място

19.	Кражба, присвояване или неправомерно използване на търговска марка и други подобни посегателства върху дейността	1. Извършване на регистрация по запазване на търговската марка 2. Маркиране на всички продукти или услуги със знака на търговската марка 3. Създаване на предпазни защити, които идентифицират уникалността на изделието 4. Завеждане на съдебни дела
20.	Кражби на активи	1. Застраховане 2. Разширяване на видеонаблюдението 3. Увеличение на физическата охрана 4. Възлагане на охраната на външни фирми 5. Физическо „застопоряване на активи”
21.	Погиване на активи, включително от природни бедствия (пожари, наводнения, земетресения)	1. Застраховане 2. Съобразяване и прилагане на правила за аварийна безопасност 3. Въвеждане на системи за ранно предупреждение и противодействие – противопожарни аларми и системи за разпръскване на вода 4. Идентифициране на природните рискове и измерване на уязвимостта към тях 5. Следене на прогнозите за бъдещи природни бедствия с оглед предприемане на спешни мерки за предпазване и съхранение на активите
22.	Повреди на ключови активи за дейността на предприятието	1. Спазване на препоръчаните срокове за поддръжка и обслужване на активите 2. Поддържане на наличност от резервни части 3. Обучение на персонала, зает с обслужването и ремонта на дълготрайни активи 4. Обучение на персонала за безопасна и правилна работа с машини, съоръжения и оборудване 5. Сключване на договор с обслужваща фирма, която да е на разположение 24 часа в денонощието
23.	Ограничаване или прекъсване на процеса на доставка на ел. енергия, вода, природен газ (по независещи от предприятието причини)	1. Използване на генератори за производство на ел. енергия – дизелови, бензинови, ветрогенератори, използване на слънчева енергия и др. 2. Използване на собствени водоизточници или използване на големи резервоари за съхранение на вода 3. Преместване на производството на места, където няма ограничения или прекъсванията на доставките са по-редки (например в селските райони рискът е много по-голям или на местата с остаряла инфраструктура) 4. Промяна на продуктите и/или процесите и намаляване на зависимостта от ел. енергия или вода (преход към ниско енергоемки и водоемки продукти и процеси)
24.	Липса на достатъчно работно пространство	1. Обмисляне на гъвкаво работно време – работа на смени или работа от вкъщи 2. Наем на нови офис площи 3. Преместване на ново работно място

25.	Текучество на кадри или липса на кадри	1. Наемане и обучение на нови кадри 2. Използване на системи за поощрения и бонуси 3. Подобряване на условията на труд 4. Провеждане на анкети и събеседване с персонала за идентифициране на проблеми 5. Преглед на заплащането в конкурентни фирми и отрасли
26.	Липса на достатъчно умения, квалификация и способности на персонала	1. Използване на правителствени програми или специализирани фирми за обучение и повишаване на квалификацията на персонала 2. Обучение на работното място от служители с необходимите умения 3. Автоматизиране на процесите на работа, с оглед намаляване на ефекта на човешкия фактор 4. Аутсорсинг на определени дейности 5. Ежегодни събеседвания и оценка на персонала
27.	Осигуряване на здравословни и безопасни условия на труд	1. Ежедневен инструктаж 2. Правила за работа с машини и съоръжения в производствените помещения 3. Обучение по въпроси, свързани с безопасни условия на труд 4. Осигуряване на работни и предпазни облекла, достъп до вода, работа вкъщи при лошо време, осигуряване на транспорт 5. Провеждане на редовни прегледи от Служба по трудова медицина 6. Разработване на процедури за докладване на инциденти
28.	Непозволено проникване в информацион-ната система и сигурност на данните, кражба на данни	1. Използване на пароли за достъп, антивирусни програми, програми за неутрализиране на зловреден софтуер, използване на криптирана връзка и протоколи за сигурност, криптиране на информацията 2. Наемане на ИТ фирма за разрешаване на проблеми със сигурността, включително провеждане на одит на сигурността 3. Дефиниране на нива на достъп на служителите според длъжностната им характеристика 4. Ежедневна проверка на ИТ системите за неоторизиран достъп 5. Ограничаване на достъпа до вътрешната мрежа през интернет
29.	Срив на информацион-ната система	1. Архивиране на информационната система 2. Процедура за възстановяване на работоспособността на информационната система 3. Използване на услугите на външни фирми, специализирани в дейността
30.	Изтичане на поверителна информация от фирмата	1. Промени в Правилата за етично поведение 2. Периодично обучение по етично поведение 3. Завеждане на съдебни искове

31.	а) Получаване на актуална счетоводна информация б) Възможност за съществуване на неотразени операции	1. Осигуряване на необходимия информационен поток към счетоводното звено; 2. Навременност на подаваната към счетоводното звено информация 3. Ежедневно осчетоводяване на всички операции съобразно нормативните изисквания и възприетата счетоводна политика 4. Ежедневно изготвяне на баланс и аналитична оборотна ведомост и активно участие при изготвяне на ежедневните справки 5. Програмни продукти за автоматизиране на процесите, систематизиране на информацията, улесняване достъпа на данните от първичните документи 6. Ежемесечен преглед от ръководството
32.	Съхранение на счетоводната информация	1. Надеждно съхраняване на хартиените носителив метални каси 2. Пароли на архивите 3. Архивиране на преносими носители, които същосе съхраняват в метални каси 4. Ясни и точни процедури за архивиране и разархивиране

- **ПРИМЕРИ И ПРАКТИЧЕСКИ НАСОКИ КЪМ ПРЕДПРИЕМАЧИТЕ:**
  - АНАЛИЗ НА РИСКОВЕТЕ И ИЗГОТВЯНЕ ОЦЕНКА НА РИСКА ЗА РАБОТЕЩИТЕ И ПОСЕТИТЕЛИ
  - ОЦЕНКА НА РИСКА ЗА ЗДРАВЕТО И БЕЗОПАСНОСТТА ПРИ РАБОТА
  - ОЦЕНКА НА РИСКА - ПЕРИОДИЧНОСТ
  - ОЦЕНКА НА РИСКА И АКТУАЛИЗИРАНЕ - В КОИ СЛУЧАИ СМЕ ДЛЪЖНИ ДА ПРЕРАЗГЛЕЖДАМЕ И КАК ДА ГО НАПРАВИМ?

ПОДОБРЯВАНЕ УСЛОВИЯТА НА ТРУД И ПРЕМАХВАНЕ /НАМАЛЯВАНЕ/ НА РИСКОВЕТЕ ЗА ЗДРАВЕТО НА РАБОТЕЩИТЕ - ОЦЕНКА НА РИСКА

- **ОЦЕНКА /ПРЕОЦЕНКА/ НА РИСКА ЗА ЗДРАВЕТО И БЕЗОПАСНОСТТА НА РАБОТЕЩИТЕ.**

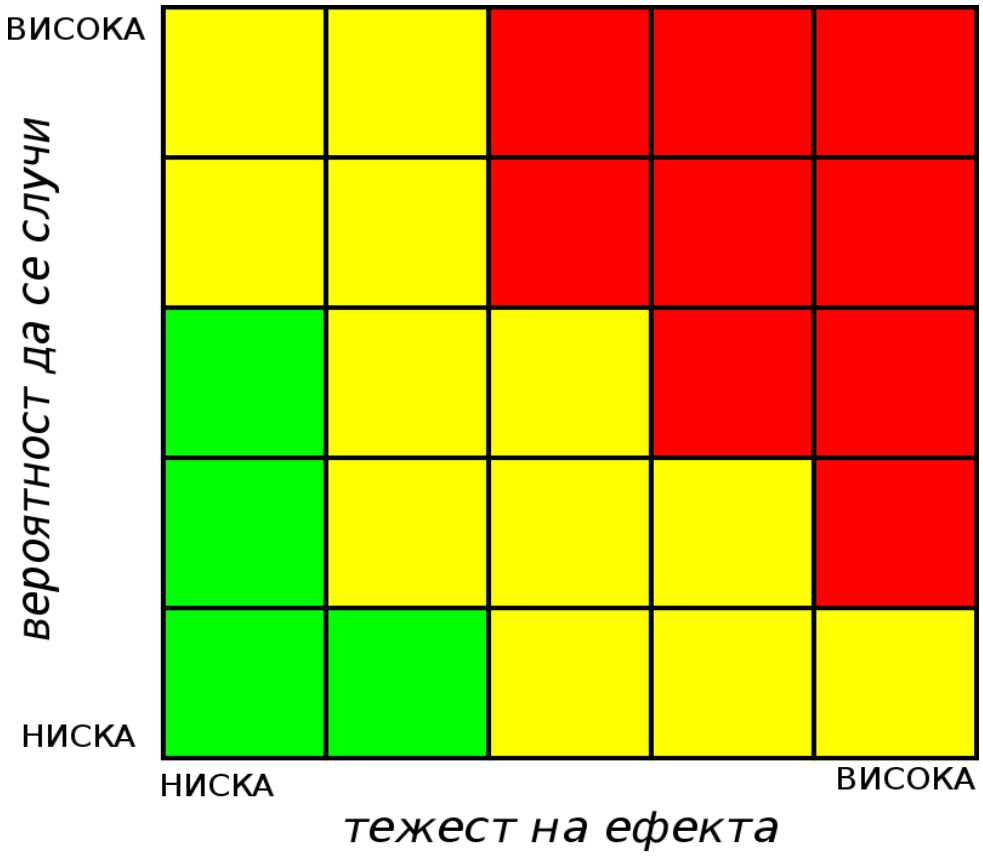
Анализ и оценка на:

- Работни помещения
- Работни процеси
- Работно оборудване
- Работни места
- Организация на труда
- Използвани суровини и материали
- Други странични фактори, които могат да породят риск

Оценка на риска за здравето при работа с високо нервно-психично напрежение и неблагоприятни психо-социални фактори, наложен ритъм и монотонност, принудителна работна поза, нерационални режими на труд и почивка.
Оценка на риска от разпространение на коронавируса (2019-nCoV).
Анализ на състоянието на работната среда и влиянието, което оказва върху здравето на работещите.
Разработване на програми за управление на професионалните рискове.
Разработване на мерки за подобряване на състоянието на работната среда и на безопасността на труда и за оптимизиране на трудовия процес.
Извършване на анкетни проучвания сред работещите и анализ на получените данни.

Предложения за въвеждане и оценка на ефективността на работата на системи и средства за отстраняване или намаляване на риска за здравето и безопасността при работа;
Участие при ново технологично оборудване и въвеждане на нови работни процеси, методи, суровини и материали с оглед определяне на потенциалния здравен риск;
Даване на препоръки по отношение на избора на средства за колективна и лична защита;
Оценка на условията на санитарно-битовото обслужване и предложение за подобряването му.
Въвеждане на физиологични режими на труд и почивка по време на работа /съгл. Наредба № 15 от 31. 05. 1999 г./.

Становище за определяне на длъжностите подлежащи на задължително застраховане - писмена консултация и изготвяне на документацията в тази връзка;
Определяне на видовете работа, за които в предприятието е необходимо установяване на намалено работно време и право на допълнителен годишен отпуск, права, задължения и отговорности на участниците в трудовия процес в тази връзка;
Организиране на дейността при прилагане на Наредба № 11 от 2005 г. определяне на условията и реда за осигуряване на безплатна храна и/или добавки към нея;



ЛЕГЕНДА:

рискът може да бъде пренебрегнат

рискът трябва да бъде анализиран

рискът трябва да бъде управляван

ОЦЕНКАТА НА РИСКА е процес на определяне на опасностите за здравето на работниците при работа в конкретни условия на въздействие на неблагоприятни фактори на работната среда и трудовия процес, на реалния или потенциален риск за увреждане на здравето в тези условия и на приемливостта на този риск.

За всяко работно място се попълва карта за оценка на идентифицираните рискови фактори. Методика за оценка на риска при работа, която определя величината на риска като произведение от трите му компонента /вероятност, експозиция, вреда/ :

P = B x E x T

P - риск

B - вероятност за настъпване на вреда

E - експозиция на рисковия фактор

T -тежест на вредата / последици /

- **ЦИФРОВ ИЗРАЗ И ГРАДАЦИЯ НА ПАРАМЕТРИТЕ:**

Вероятността за нанасяне на вреда се преценява по: честотата, продължителността и спецификата на експозиция; вероятността от възникване на опасно събитие; техническите възможности за ограничаване или избягване на вредата; човешките възможности за ограничаване или избягване на вредата; /квалификация, опит, практически знания и умения, взаимодействие между хората, психологически, социални и ергономически аспекти и др./, стойността на параметрите на работната среда.

Вероятност (В)

0.1 Едва забележима
0.2 Практически невъзможна
0.5 Малко възможна
1.0 Малко възможна, но възможна в ограничен случай
3.0 Ниска вероятност
6.0 Напълно възможна
10.0 Относително висока вероятност

Честотата на експозиция се градира по следния начин:

Честота на експозиция (Е)
0.5 Твърде ниска (по-малко от 1 път месечно)
1.0 Много ниска (до 1 час седмично)
2.0 Ниска (до 1 час на ден)
3.0 Средна (до 1/3 от работното време)
6.0 Достатъчно висока (половината работно време)
10.0 Непрекъснато, през цялото работно време

Тежестта на вредата се преценява съобразно: вида на обектите подлежащи на защита /хора, имущество, работна и околна среда/; тежестта на възможните наранявания или увреждания на здравето; обхвата на вредата.

Последици (вреди) П
1.0 Малки Нараняване без загуба на временна работоспособност
3.0 Значителни Нараняване със загуба на временна работоспособност
7.0 Сериозни Инвалидност; необратимо нараняване
15.0 Опасни Възможен до 1 смъртен случай
40.0 Катастрофални Възможни много смъртни случаи

На базата на горните параметри и посочената формула се прави класация на риска:

Риск(Р)

1 До 20 Твърде ограничен, приемлив риск
2 От 20 до 70 Неголям /овладян/ риск, необходимо е внимание
3 От 70 до 200 Необходими са мерки за намаляване на риска
4 От 200 до 400 Необходимо е незабавно подобрение на условията на труд
5 Над 400 Прекратяване на дейността до отстраняване на риска

Оценката на риска е краен резултат, който установява допустимостта на риска и необходимостта от прилагане на мерки за неговото предотвратяване или намаляване и ограничаване. Тук трябва да се вземе под внимание и ефективността на вече приложените мерки за намаляване на риска.

- **ОПИСАНИЕ НА МЕРКИТЕ, КОИТО СЕ ВЗЕМАТ:**

На този етап трябва да се прецизират мерките, които е необходимо да се предприемат с оглед отстраняване или ограничаване на риска. Тази фаза от оценката има за цел да осигури добра защита на работещите. За да се реализира това следва да се приложат мерки, намиращи се най-високо в йерархията на превенцията:

Йерархия на превенцията

1 Избягване на рисковете
2 Заместване на опасни субстанции и ситуации с по-малко опасни или безопасни
3 Борба с риска при източника на възникването му
4 Използване на средства за колективна защита
5 Използване на средства за индивидуална защита

Оценката завършва с определяне на приоритетите и разработване на програма за изпълнение на необходимите мерки.

Типове решения, които се очакват в края на оценката на риска и предприети мерки

Степен на риска Решения Действия

Първа

P < 20 Рискът е незначителен и не се предполага, че ще нараства в близко бъдеще Не са необходими мерки

Втора

20<P<70 Рискът е овладян на приемливо ниво, но би могъл да се увеличи в бъдеще. Това е възможен риск, но няма доказателства, че би могъл да доведе до нарастване или заболяване. Сравнение на съществуващи-те мерки с приемливите практически норми и как са ситуирани в йерархията на превенцията. Ако сравнени-ето е неблагоприятно, следва да се подобрят мерките за защита.

Трета

70<P<200 Незадоволително и неефективно овладян риск Рискът следва да се отстрани

Четвърта

200<P<400 Повишен риск, който е незадоволително и неефективно овладян Незабавно се вземат и се прилагат мерки

Пета

P>400 Голям риск, неефективно овладян Прекъсва се дейността. Прилагат се незабавно мерки.

- **КРЕДИТЕН РИСК**

Кредитен риск е рискът от загуба поради неплащане на задълженията на длъжник на заем или кредитна линия (или друг вид дълг) и коя да е част от него – главница, лихва или всичко.

От кредитор към потребител

Повечето кредитори използват собствени модели за да класифицират потенциални и съществуващи клиенти според техния риск и после използват определени стратегии. С продукти като свободни потребителски кредити или ипотечни кредити, кредиторите слагат по-висока цена на капитала за по-високо рискови клиенти и обратното. С револвиращи продукти като кредитните карти и овърдрафти, рискът се контролира чрез внимателно използване на кредитните лимити. Някои продукти също така изискват обезщетения, обикновено под формата на някаква собственост.

От кредитор към бизнеса

Кредиторите може да използват възможността за размяна на цената/преимуществата на заема според неговия риск и лихвените равнища. Все пак, лихвения процент не е единствения метод да компенсира за различни нива на риск. Допълнителни условия могат да бъдат включени в договора за да позволяват на кредитора да упражнява различни нива на контрол. Подобни допълнителни условия могат да:

- ограничат кредитополучателя да отслабва балансовите си стойности във финансовите отчети. Това може да стане чрез разпродажба на активи, изкупуване обратно на акции, плащане на дивиденти и т.н.;
- позволяват за следене на дълга, изискване за одит, месечни отчети и т.н.;
- позволят на кредитора да изисква дълга при определени условия, обикновено базирайки се на определени случаи, или когато определени финансови показатели преминат дадени граници на техните стойности.

Сравнително нов начин за предпазване на кредиторите от и собствениците на облигации от опасностите от неплащане са кредитните деривати, най-обикновено под формата на кредитни суапове. Тези финансови инструменти позволяват на кредиторите да закупят защита от неплащане от трети лица. Тези трети лица получават периодична такса (кредитния спред) като компенсация за риска, който поемат и се съгласяват да закупят дълга в случай на неплащане.

От бизнеса

Компаниите носят този риск когато не изискват първоначално или на момента плащане за продукти или услуги. Когато една компания първо доставя продуктите и/или услугите и изисква плащане след това, тя автоматично носи риска от не получаване на плащането от клиента за периода от доставка до получаване на средствата.

За да се справят с риска, много компании използват налични ресурси или използват трети компании. Налични ресурси могат да са бази данни създадени въз основа на личния опит, определени програми определящи риска чрез математически/статистически изчисления. Информация за определен клиент може да бъде черпена от кредит рейтингови агенции като Мудис, Стандарт енд Пуър и тн. Кредитния риск за малки компании практически не е

възможно да се управлява, главно поради липсата на информация и недостатъчното ресурси. Поради тази причина, малките компании са по-вероятни потърпевши от неплащания на техни клиенти и т.н.

От физически лица

Потребителите могат да търпят последствията от кредитния риск директно като депозитори в банки или в ролята си на инвеститори/кредитори. Също така, те могат да се сблъскат с кредитен риск, когато влизат в стандартна сделка, в която се предоставя депозит на отсрещната страна, например за голяма покупка или за договор за наем и тн. Работниците на всяка фирма също така носят кредитния риск на работодателя си от неплащане на техните заплати.
В някои случаи, правителствата могат да приемат, че способността на физическите лица да оценяват кредитния риск е ограничена и същия този риск може да ограничи икономическата ефективност. Във връзка с това, правителството на коя да е държава може да приеме определени законови мерки или механизми, които да предпазят потребителите от някои от тези рискове. Пример за това са банковите депозити, които в много страни са застраховани (гарантирани) от централната банка до определена сума, което, за депозитори до тази сума, премахва нуждата за оценяване на кредитния риск на тази определена банка.

- **ПАЗАРЕН РИСК**

Пазарен риск е рискът, че цената на една инвестиция ще намали поради промени в някои пазарни фактори. Четирите стандартни пазарни фактора са:

- *риск на ценни книжа*, или риска, че цената на ценните книжа (акции, облигации и тн) ще се промени.

Рискът на ценни книжа е рискът, че нечии инвестиции ще намалят стойността си заради промени в пазара на ценни книжа по един или друг начин.
Мярка за риска на ценни книжа е обикновено стандартната девиация на цената на дадените ценни книжа, върху определен брой периоди. Стандартната девиация ще очертае нормалните флуктуации, които могат да бъдат очаквани за тези определени ценни книжа и под средните стойности. Все пак, след като повечето инвеститори няма да приемат флуктуации над средните нива за риск, някои икономисти предпочитат други методи за измерването му.

- лихвен риск, или риска, че лихвените нива ще се променят.
- валутен риск, или риска, че валутните курсове ще се променят.
- продуктов риск, или риска, че цените на определени продукти (например зърно, метали, кафе и т.н.) ще се промени.

Понякога като пети допълнителен фактор се включва:

- риск на индекс на ценни книжа – рискът, че индекс на ценни книжа или друг индекс ще се промени.

Измерване
Пазарният риск обикновено се измерва, като се използва VaR (Value at Risk) методологията. Тя е добре известна като рисковоопределяща техника, но съдържа определен брой

ограничаващи предположения, които ограничават нейната точност. Първото предположение е, че съставките на портфейла остават непроменени за единичния период на модела. За кратки периоди това ограничаващо предположение се смята за приемливо. За по-дълги периоди много от трансакциите могат да достигнат падеж през периода на моделиране. Стресови парични потоци, прикрепени опции (embedded options), промени в нивата на плаващи лихвени проценти и др. са игнорирани в тази техника за моделиране на единични периоди.

Пазарният риск може да се разграничи от специфичния риск, който измерва риска от намаляване на нечия инвестиция заради промени в определена индустрия или сектор за разлика от промяна в целия пазар.

Value At Risk
Value at Risk е мярка за риска от загуба при инвестиции. Това е стандартна мярка за риск на даден актив или портфолио от активи във финансовата математика и финансовия мениджмънт на риска.

Value at Risk (VaR) се изчислява за определен интервал от време, за определен актив и зададена вероятност. VaR от 10 млн. лева при вероятност 99% и времеви хоризонт от един ден означава, че вероятността активът да загуби повече от 10 млн. лева за един ден е 1%.

Макар VaR да е стандартната мярка за риск използвана от бизнеса съществува критика към използването ѝ. От теоретична гледна точка е важно, че VaR не е субадитивен, тоест на теория е възможно VaR на портфолио да е по-голям от сумата на VaR на отделните му съставни части (което противоречи на CAPM). Практически проблеми има при моделирането на данните, което е свързано с несигурност.

- **СТАНДАРТИ ЗА УПРАВЛЕНИЕ НА РИСКА**

ISO 31000:2018 УПРАВЛЕНИЕ НА РИСКА. УКАЗАНИЯ

Международният стандарт **ISO 31000** осигурява принципите и общите насоки за управление на риска. Стандартът може да се използва от всяка публична, частна или обществена организация, предприятие, асоциация, група или отделна личност. Ето защо, този международен стандарт не е насочен към определена индустрия или сектор. Той може да се прилага за целия период на съществуване на организацията и на широк спектър от дейности, включително стратегии и решения, дейности, процеси, функции, проекти, продукти, услуги и ресурси.
Този международен стандарт може да се прилага за всички видове риск, независимо от техните характеристики, както и независимо дали са с положителен или отрицателен ефект. Въпреки, че **ISO 31000** дава общи насоки той няма за цел да насърчава еднаквото управление на риска в различните организации. При разработването и прилагането на планове за управление на риска и организационна рамка трябва да се вземат под внимание специфичните потребности и цели, конкретните обстоятелства, структурата, дейностите,

процесите, функциите, проектите, продуктите, услугите, или активите както и използваните конкретни практики.
Стандартът е предназначен да се използва за координиране на процесите на управление на риска в съществуващите и бъдещите стандарти. Той осигурява общ подход и подкрепа за стандарти, разглеждащи специфични рискове и / или сектори, и не замества тези стандарти. **ISO 31000** не е предназначен за целите на сертификацията.
ISO 45001:2018 (БДС ISO 45001:2018) СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ЗДРАВЕТО И БЕЗОПАСНОСТТА ПРИ РАБОТА
ISO 45001

Област на приложение:

ISO 45001 е международен стандарт, който определя изискванията за система за управление на здравето и безопасността при работа като дава насоки за неговото прилагане и по този начин дава възможност на дадена организация да подобри резултатите си при предотвратяване на наранявания и заболявания, причинени от условията на работната среда.

ISO 45001 е приложим за всяка една организация, която желае да създаде, внедри и поддържа система за управление на ЗБР, за да подобри здравето и безопасността при работа, да премахне или намали до минимум рисковете за ЗБР (включително недостатъците на системата), да се възползва от възможностите за ЗБР и отстрани несъответствията на системата за управление на ЗБР, свързани с нейните дейности. Всички изисквания на стандарта могат да бъдат интегрирани в процесите на управление на организацията.
Стандартът е приложим за всяка организация, независимо от нейната големина, вид и дейности, Той е приложим спрямо рисковете за ЗБР, които са под управлението на организацията, като се вземат предвид фактори като контекста, в който функционира организацията, потребностите и очакванията на нейните работници и на други заинтересовани страни.

ISO 45001 позволява на организацията да интегрира чрез своята система за управление на здраве и безопасност при работа, други аспекти на здравето и безопасността, като например благосъстоянието на своите служители.

ISO 45001 не определя конкретни критерии за безопасността при работа и не предвижда изисквания за концепцията на системата за управление на здравето и безопасността на работното място. Системата за управление на организацията трябва да бъде специфична спрямо нейния контекст, за да посрещне собствените ѝ нужди за предотвратяване на наранявания и заболявания на служителите.

ISO 45001 не разглежда конкретно въпроси като безопасността на продукта, имуществените щети или въздействие върху околната среда, а самата организацията не е задължена да взема предвид тези въпроси, освен ако те не представляват риск за нейните служители.

ISO 45001 не е правно обвързващ документ, а е инструмент за управление, който организациите могат да използват доброволно, ако желаят да премахнат или да сведат до минимум опасните рискове за здравето и безопасността на своите служители.

Системата за управление на здравословните и безопасни условия на труд, базирана на **ISO 45001**, спомага за подобряване на условията на работната среда чрез:
• разработване и прилагане на политика и цели по здраве и безопасност;
• разработване и прилагане на политика и цели по здраве и безопасност;
• създаване на систематични процеси, които да отчитат "контекста" и които вземат под внимание рисковете и възможностите за организацията, както и правните и други изисквания;
• определяне на опасностите и рисковете за здравето и безопасността, свързани с дейността, с цел тяхното премахване или свеждане до минимум на потенциалните им последици;
• създаване на оперативен контрол за управление на рискове по здраве и безопасност, както и тези, свързани с правните и други изисквания;
• повишаване на осведомеността за рисковете, свързани със здравето и безопасността;
• оценяване на изпълнението на изискванията по здраве и безопасност и търсене на подходящи мерки за подобряване на системата;
• осигуряване на активна роля на служителите при разрешаване на проблемите, свързани със здравето и безопасността при работа.

Ползи от внедряване на ISO 45001:
В съответствие с политиката по ЗБР на организацията, очакваните резултати от внедряването на системата за управление на ЗБР включват:
• постоянно подобряване на резултатността по ЗБР;
• изпълнение на законови и други изисквания;
• постигане на целите по БЗР.

Комбинацията от горе посочените мерки ще подобрят репутацията на организацията, както и биха могли да допринесат за:
• по-добра способност за реагиране по отношение на законовото съответствие;
• намаляване на общите разходи от инциденти на работното място;
• намаляване разходите от прекъсванията в производството;
• намаляване на разходи за застрахователни премии;
• намаляване на отсъствията и текучеството на персонала.

ISO 45001 следва структурата, възприета в други ISO стандарти за управление, като например **ISO 9001** и **ISO 14001**. При разработването на стандарта са взети предвид също и други международни стандарти (**OHSAS 18001** и ILO-OSH на Международната организация на труда), национални стандарти, както и Международните трудови стандарти и конвенции (ILS).

Внедряването на **ISO 45001** е сравнително лесно, особено за онези организации, които имат вече система за управление на здравето и безопасността при работа и е лесно да хармонизират и **интегрират** изискванията на **ISO 45001** с другите ISO стандарти за управление.

Как да внедрим ISO 45001? (Реализация на системи за управление)

ISO 45001:2018 (БДС ISO 45001:2018) Системи за управление на здравето и безопасността при работа

- **СИСТЕМИ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА**

Системата за управление на сигурността на информацията (**ISMS**) е подход за управление на чувствителната за организацията информация по начин, който гарантира запазването на нейната сигурност. Тази информация може да бъде фирмена - ноу-хау, лични данни, както и собственост на клиента.
Международният стандарт **ISO 27001** поставя изисквания към **Системите за управление на сигурността на информацията** (ISMS).
ISO 27001 е приложим за всякакви видове организации: търговски, нетърговски, правителствени и неправителствени.
Предимствата от внедряването на **Система за управление на информационната сигурност**:

- определяне на изискванията и целите на сигурност;
- гарантиране, че организациите изпълняват законодателството и други регулативни изисквания;
- гарантиране, че информационният риск се управлява ефективно, от гледна точка на средства;
- определяне на нови процеси за управление на информационната сигурност;
- оценяване на съществуващите процеси за управление на информационната сигурност;
- установяване на съответствие от вътрешни и външни одитори в организациите с политиките, нормативната уредба и приложимите стандарти;
- предоставяне на клиентите на съответната информация за информационната сигурност.

За да съхрани информацията си, организацията трябва да предприеме следните стъпки:

- дефинира политика по информационната сигурност;
- да идентифицира и оцени рисковете за сигурността;
- да определи и внедри подходящи контроли за сигурността на информацията.

Стандарт **ISO 27001** изисква стриктно спазване на съответните законови, подзаконови и договорни задължения свързани със сигурността на информацията, оптимизирано използване на наличните ресурси, както и периодични вътрешни проверки на системата с цел непрекъснато усъвършенстване.

Друг стандарт за сигурност, много сходен на **ISO 27001** , е PCI DSS.

PCI DSS (Payment Card Industry Data Security Standard) представлява **стандарт за сигурност** за търговци и процесори на платежни карти и е жизнено важен за прилагането на информационната сигурност и най-добрите практики в индустрията с кредитни карти.

PCI DSS е разработен от PCI SSC (PCI Security Standards Council). PCI Security Standards Council е отворен глобален форум, чието начало в поставено през 2006 г. PCI SSC е отговорен за развитието, управлението, образованието и информираността по стандарти за сигурност PCI.

PCI DSS е основан от пет световни марки за разплащане - American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc, които са се споразумели да включат PCI DSS като техническо изискване за съответствие с всяка от техните програми за сигурност на данните.

Изискванията на PCI DSS могат да бъдат напълно интегрирани с изискванията на **ISO 27001** като бъдат обединени в една обща система.

Сертификацията на **Система за управление на сигурност на информацията**, съгласно **ISO 27001** и PCI DSS доказва, че Вашата организация гарантира в максимална степен сигурността, както на собствената си информация, така и на тази на своите клиенти.

Внедрената и функционираща **Система за сигурност на информацията (ISMS)** ще гарантира също така осигуряването на непрекъсваемостта на Вашия бизнес, в случаи на извънредни ситуации и кризи.