АНАЛИЗ НА ПОДХОДИ ЗА ОЦЕНКА НА РИСКА И РАЗРАБОТКА НА МОДЕЛ ЗА ОЦЕНКА НА РИСКА ЗА ИНТЕГРИРАНА ВЪТРЕШНА УПРАВЛЕНСКА СИСТЕМА

Кристиан Томов

ANALYSIS OF A RISK ASSESSMENT APPROACHES AND THE DEVELOPMENT OF AN INTEGRATED INTERNAL MANAGEMENT SYSTEM RISK ASSESSMENT MODEL

Kristian Tomov

Резюме: Понастоящем бизнес светът непрекъснато се променя и всеки ден става по-сложен и по-комплексен. По своята същност, той е изпълнен с риск. През последните години, повишаването на регулаторните изисквания принуди фирмите да изразходват огромни ресурси за справяне с проблемите на риска. Правилно съставена, оценката на риска дава на организациите ясна представа за състоянието на рисковете в бизнес процесите, независимо дали са вътрешни или външни, непосредствено предстоящи или по-далеч напред в бъдещето. Процесът на оценка на риска, приложен последователно в цялата организация, дава възможност за по-добро управление, идентифициране, оценяване и третиране на рисковете за бизнеса. В настоящата работа са разгледани конкретни въпроси, свързани с анализ и оценка на риска, приложими в телекомуникационни структури.
Ключови думи: анализ и оценка на риска, управление на риска, модел за оценка на риска, приемане, прехвърляне или третиране на риска

Abstract: Currently, the business world is constantly changing and every day becomes more complicated and more complex. In essence, it is fraught with risk. In recent years, increasing regulatory requirements force companies to spend resources to deal with issues of risk. Properly constituted, risk assessment gives organizations a clear picture of the status of risks in business processes, whether internal or external, imminent or far into the future. The process of risk assessment applied consistently throughout the organization enables better management, identification, assessment and treatment of risks to the business. The present work deals with particular issues related to the risk assessment applied in telecommunication structures.
Keywords: analysis and risk assessment, risk management, model risk assessment, acceptance, transfer or risk treatment

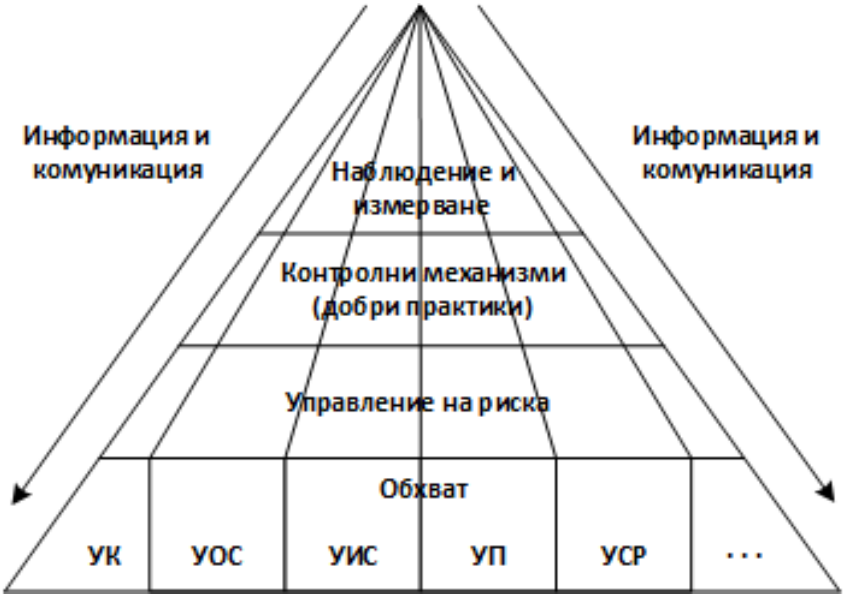
ВЪВЕЖДАНЕ В ПРОБЛЕМАТИКАТА

Понастоящем бизнес светът непрекъснато се променя и всеки ден става по-сложен и по-комплексен. По своята същност, той е изпълнен с риск. Исторически погледнато, фирмите са гледали на риска като на необходимо зло, което трябва да бъде сведено до минимум или смекчено, когато това е възможно. През последните години, повишаването на регулаторните изисквания принуди фирмите да изразходват огромни ресурси за справяне с проблемите на риска, тъй като акционерите на свой ред контролират дали фирмите имат надеждно управление на корпоративния риск. Увеличеното търсене на прозрачност около съществуването на риска не винаги е изпълнено. В настоящата глобална икономическа среда, идентифициране и управление на риска в рамките на една организация, става все по-важно за успеха и в дългосрочен план. Правилно съставена, оценката на риска дава на организациите ясна представа за състоянието на рисковете в бизнес процесите, независимо дали са вътрешни или външни, непосредствено предстоящи или по-далеч напред в бъдещето. Една добра оценка е „закотвена” в апетита към риск на организацията, което осигурява база за определяне на рискови реакции. Процесът на оценка на риска, приложен последователно в цялата организация, дава възможност за по-добро управление, идентифициране, оценяване и третиране на рисковете за бизнеса. Това изисква внедряване и поддържане на необходимия контрол във всички сфери на бизнеса (процеси, качество, околна среда, сигурност, производство

и др.), за да се гарантират качествени и ефективни операции с едновременно спазване на регулаторните изисквания.

2. ДЕФИНИЦИЯ И АНАЛИЗ НА ПРОЦЕСА „ОЦЕНКА НА РИСКА“

Оценката на риска е систематичен процес за идентифициране и оценка на събития (т.е. възможните рискове и заплахи), които биха могли да повлияят отрицателно на постигането на корпоративните цели. Такива събития (събитие „идентифицирана поява на състояние в процес, услуга, система или мрежа, показваща възможно нарушаване на корпоративните оперативни правила (изисквания на интегрирана вътрешна управленска система (ИВУС), пробив на контролен механизъм или неизвестна до момента ситуация засягаща оперативната дейност)“ [1]) могат да бъдат идентифицирани в бизнес средата (например, икономически тенденции, регулаторните изисквания, конкуренцията и др.) и в рамките на вътрешно корпоративната среда (например, хора, процеси, инфраструктура и др.) на организацията. Когато тези събития се пресичат с организационните цели, тогава възникват рискове. Затова рискът се дефинира като „възможността, че дадено събитие ще се случи и че ще възпрепятства постигането на целите до някаква степен”. Качествено разработеният и внедрен процес за управление на риска формира фундамента за корпоративно интегрирано управление на риска на ИВУС, което е и изискано от международно признат и прилаган стандарт COSO Enterprise Risk Management - Integrated Framework (Комитет на спонсориращите организации) [2]. Важно е да се разбере взаимовръзката между корпоратината оценка на риска, контролните механизми и наблюдението на ефективността. За по-лесно разбиране на гореописаното е показан модел на ИВУС с интегриран процес за управление на корпоративния риск – фиг. 1.



Фиг. 1. Модел на ИВУС [3].

На фиг. 1 са използвани следните съкращения по отношение на основната структура и основните параметри на модела на ИВУС:

Наблюдение и измерване – извършва се непрекъснато наблюдение и измерване на параметрите на ИВУС от старшия управленски състав. Това включва вътрешно одитиране, документиране на резултати, наблюдение и оценка на тяхното развитие, измерване на тяхната оперативна и финансова ефективност.

Контролни механизми (добри практики) – съвкупност от организационни и технически контролни механизми (превантивни, детективни и коректривни), използващи приети добри практики.

Управление на риска – модел за управление на цялостния корпоративен риск.

Обхват – обхват на прилагане на отделните сфери в модела на ИВУС

УК - управление на качеството

УОС - управление на околната среда

УИС - управление на информационната сигурност

УП - управление на процесите на взаимодействие

УСР - управление на сигурността по време на работа

…- управление на непрекъсваемостта и управление на съответствието спрямо законодателството (за определените сфери)

Информация и комуникация – посока на движение на информацията и комуникацията

Видове корпоративни активи

Предлага се разглеждането на 13 категории корпоративни активи като част от оценката на риска, описани в табл. 1 [ISO/IEC 27005, Information technology - Security techniques - Information security risk management]. Процесът на определяне на активи е приведен в съответствие с изискванията за сигурността на ISO/IEC 27001:2013.

Табл. 1. Пример за видове активи на телекомуникационна структура.

ТИП АКТИВ	ПОЯСНЕНИЕ
Процеси	Състои се от набор от логически свързани индивидуални задачи (операции) с цел извършване и постигане на бизнес или оперативна цел.
Продукти/услуги	Корпоративни продукти и/или услуги.
Сгради и обекти	Инфраструктура (обработка на данни и съответни съоръжения – изчислителни центрове, административни, производствени и др.)
Физическа сигурност	Контролни механизми за физическа сигурност (видео, картова система, охрана и др.)
Доставчици	Критични и некритични трети страни - доставчици, които предоставят средства за поддържане на операциите на бизнеса, на мрежите, системите, услугите или продуктите на компанията.
Информационни и комуникационни системи	Системи и мрежи.
Корпоративна документация	Например оперативна, финансова, техническа, процесна и др.
Клиенти, решения и продукти	Данни за клиента и документация за консумирани услуги и продукти (решения), статистически данни и др.
Човешки ресурси	Човешки ресурси на компанията.

Видове събития

Събитията могат да бъдат категоризирани по различни начини. Например, те могат да бъдат обединени в една матрица, с хоризонтални редове посочващи категории рискови коренни причини и вертикални колони, представляващи процеси на бизнеса или

функционални области. Всички приложими области на възникване на риск могат съответно да се отбелязват. Друг подход се състои в улавяне на всички съответни видове събития и свързване на тези с по-широките категории, както е показано в табл. 2.

Табл. 2. Пример за категоризиране от гледна точка на външни и вътрешни събития.

Събития	**Групи**	**Източник**			
Външни	Икономически	Разпад на финансови пазари	Безработица	Сливания и придобивания	Конкуренция
	Политически	Промяна на законодателство			
	Околна среда	Бедствия	Изисквания за рециклиране		
Вътрешни	Инфраструктура	Наличност на активи	Способност на активите	Достъп до активите	Сложност на активите
	Човешки ресурси	Наличност на персонал	Способности на персонала	Сигурност по време на работа	Измамни дейности
	Процеси	Капацитет	Дизайн	Изпълнение	Зависимости спрямо доставчици
	Технологии	Интегритет, конфиденциалност, наличност на данните и ИКТ системи/мрежи.	Разработка и внедряване	Поддръжка	

Типове оценки на риска в интегриранта система за оценка на риска

Оценката на риска може да се проведе на различни нива (топ мениджмънт, среден мениджмънт и др.) и сфери (управление на качеството, доставяне на услуги и др.) на организацията. Целите и събитията, които се обсъждат, определят обхвата на оценката на риска, както и дейности, които трябва да бъдат предприети след анализ на неприемливия риск. Примери за често извършвани оценки на риска включват:

- *Стратегическа оценка на риска* [4]. Оценка на рисковете, свързани с мисията на организацията и стратегическите цели, обикновено се извършва от висшите управленски екипи в рамките на срещите на стратегическото планиране, с различна степен на формалност.
- *Оперативна оценка на риска [5]*. Оценка на риска от отпадане на оперативна дейност, произтичаща от неадекватни или недобре функциониращи вътрешни процеси, хора и системи, или от външни събития. В някои индустрии, регулаторите са наложили изискването спрямо компаниите редовно да идентифицират и докладват рисковете и мерките за превенцията им.
- *Оценка на риска от измами [6]*. Оценка на потенциалните случаи на измама, които могат да окажат влияние върху етиката на организацията и стандартите за съответствие, изискванията на бизнес практиките, финансовото отчитане, почтеността, както и други цели. Подобна оценка на риска се извършва често поради изисквания на стандарти и държавни изисквания, като например Sarbanes-Oxley-Act (SOX) и EuroSOX. Този тип оценка обикновено се извършва на ниво функции поръчки, счетоводни действия и продажби.

- *Оценка на клиентския риск [7]*. Оценка на риска от клиенти и свързани събития, които потенциално биха могли да окажат влияние върху репутацията и финансовата позиция на организацията. Тази оценка включва, например, намерения на клиента, кредитоспособността и други релевантни фактори. Тази обективна оценка се извършва от клиентските мениджъри.
- *Оценка на пазарния риск [8]*. Оценка на движенията на пазара, които могат да влошат работата или да изложат на риск организацията, като се имат предвид лихвен риск, валутен риск и стоков риск. Това обикновено се извършва от специалисти по пазарния риск.
- *Оценка на риска на продукта (и съответно на проекта) [9]*. Оценка на рисковите фактори, свързани с продукти или услуги на организацията, от проектирането, разработка и производство на продукт или доставка на услуга, дистрибуция, използване (цикъл на живот на продукта), унищожаването и рециклирането му. Тази оценка има за цел да се разбере не само въздействие върху приходите или разходите, но също така и въздействието върху марката, взаимовръзки с други продукти/услуги, зависимостта от трети страни, както и други значими фактори (качество, ефект спрямо околната среда, сигурността по време на работа, процесите за доставка на продукта или услугата и правното съответствие на продукта или услугата). Този тип оценка обикновено се извършва чрез управлението на продуктовите групи или управление на доставка на услуги.
- *Оценка на риск, произлизащ от веригата за доставки и аутсорсинг* [10]. Оценка на рисковете, свързани с доставка на компоненти от трета страна с цел създаването на продукти и услуги, включително подбор и управление на доставчици. Много компании работят на принцип „Just in Time“ (доставка на нужни компоненти в точно определен момент на нуждата им), което води до многобройни преки зависимости от трета страна. Оценката включва и аутсорсинг услуги закупени от организацията и пряко свързани с оперативната дейност.
- *Оценка на риска за сигурност (включващо физическа сигурност и логическа сигурност на корпоративни активи)* [11]. Оценка на потенциални нарушения на процеси, активи (сгради, информационни и комуникационни технологии) и информация за защита, непрекъсваемост и сигурност на организацията. Това включва инфраструктура, приложения, процеси и операции, хора и др. Обикновено се извършва чрез функция „информационна сигурност“.

Примерите, описани по-горе, са само илюстративни. Всяка организация трябва да прецени какви видове оценки на риска са свързани с нейните цели и дейност. Такова определение може да бъде направено чрез анализ на ИВУС и сферите ѝ на дейност. Обхватът на оценката на риска, зависи от заложените приоритети и цели. Обхватът може да бъде малък и специфичен спрямо особен риск, както в някои от примерите по-горе. Той може да бъде широк, на високо ниво: например, оценка на риска за корпоративно ниво на зрялост на процесите или в детайли за всеки корпоративен актив. Изборът се влияе от ресурсите и мотивацията на организацията да оценява правилно риска и да може да го управлява.

Основа на корпоративната оценка на риска

За да бъде ефективна, оценката на риска не може да бъде просто един списък или процес, който е изключен от процеса на вземане на бизнес решения. Вместо това, тя трябва да бъде интегрирана в управленския бизнес процес и сферите му, по начин, който да осигурява навременна и актуална информация за рисковете и тяхното управление. Оценката на риска, трябва да бъде един непрекъснат процес, той трябва да бъде

управляван от бизнеса и да се вгражда в рамките на работния цикъл, веднага когато се започне със стратегическо планиране, осъществявано чрез бизнес процесите и завършва с оценка, както е показано в табл. 3.

Когато процесът за оценка на риска е включен в текущите бизнес практики, оценката на риска може да се управлява като част от процеса за вземане на решение, ден за ден, по начин, съвместим с апетита към риск на организацията. Оценката на риска трябва, например, да се задейства в рамките на работния процес, когато възникват особени обстоятелства извън текущия бизнес цикъл, например - промени в работната среда, оценка на нови проекти, въвеждане на нови продукти или инвестиции, разширяване на нови пазари, технологични промени, променени правни изисквания, както и корпоративни преструктурирания.

Табл. 3. Бизнес цикъл на примерна телекомуникационна компания.

	ФАЗА 1 - СТРАТЕГИЯ	**ФАЗА 2 – ПРОЦЕСИ И ИЗПЪЛНЕНИЕ**	**ФАЗА 3 – ОЦЕНКА НА РИСКА**
Ключови фази на бизнес цикъл	Бизнес стратегия и планиране	Бизнес процеси и тяхното изпълнение	Оценка
Ключови контролни механизми	Организационни контролни механизми	Организационни и технически контролни механизми	Докладване на анализ на риска в различните оперативни функции
Оценка на риска	• Изрично интегриране на риска в стратегическите планове • Определяне апетита към риск и да се осигури неговата съгласуваност със стратегията • Разпределяне на икономическия капитал по бизнес единици/рискови дейности • Определяне на бизнес и индивидуални цели за изпълнение	• Изрично интегриране на риска в стратегическите планове • Определяне на склонността към риск и да се осигури нейната съвместимост със стратегията • Разпределение на икономическия капитал по бизнес единици/предприятия • Идентифицира не на бизнес и индивидуални цели за изпълнение	• Доклад с резултати и препоръки.

Способността да се идентифицират, оценяват и управляват рискове е често показателно за способността на организацията да реагира и да се адаптира към промените в бизнес средата или в самата компания.

Оценката на риска следователно помага на организациите бързо да разпознаят потенциални неблагоприятни събития, да бъдат по-активни и далновидни и да създадат подходящи реакции спрямо риска, като по този начин намаляват изненадите и разходите или загубите, свързани с бизнес прекъсвания.

Това е мястото, където реалната стойност на оценката на риска се намира: в предотвратяването или минимизирането на негативните изненади и разкривайки нови възможни рискове.

Основни принципи за ефективно прилагане на модел за оценяване на риска

За да се получават смислени и ценни резултати от процеса за оценка и управление на риска, е нужно спазването на минимални изисквания спрямо прилагането на модела в оперативната корпоративна среда:

1. Управлението на процеса за оценка на риска, трябва да бъде ясно дефинирано и документирано. Надзорът и отчетността на процеса на оценка на риска е от решаващо значение, за да има гаранция, че необходимите ресурси са обезпечени. Процесът на оценката на риска трябва да бъде внедрен в управленското ниво на организацията и трябва да бъде поддържан пряко от това ниво, за да може да се счита, че рискове се оценяват чрез строго регулиран и непрекъснат процес и че необходимите коригиращи действия са възможни и могат да бъдат предприети.

2. Оценката на риска започва и завършва с конкретни цели. Рисковете са идентифицирани и измервани във връзка с целите на организацията или, по-конкретно, за постигане на целите в обхвата на оценката на риска (както е описано по-горе). Изисква се от организацията дефиниране на цели, които са конкретни и измерими и покриват различните нива на организацията. Оценка на рисковете по отношение на тези цели улеснява преразпределението на ресурсите, необходими за управление на тези рискове и най-доброто постигане на поставените цели.

3. Рисковият рейтинг, трябва да бъде определен в количествено и/или качествено отношение. Рисковете обикновено се измерват по отношение на тяхното въздействие и вероятността им за настъпване. Времевият хоризонт, използван за оценка на вероятността за риск, следва да бъде в съответствие с времевите хоризонти, свързани с целите. Количествените рейтингови скали позволяват по-голяма степен на точност и измеримост на процеса на оценка на риска. Въпреки това, те се нуждаят от качествена гледна точка, която да може да се използва, когато рисковете не се поддават на количествено определяне, когато достоверни данни не са на разположение или когато получаването и анализирането на данни не е икономически ефективно.

Организациите обикновено използват следните мащаби за измерване на риска: редни, интервални и/или съотносителни. Редните мащаби определят ранга, реда на важност (например, ниска, средна или висока), интервалните мащаби имат числено разстояние (например, най-ниското е равно на 1, а най-високото е равно на 3, но при това най-високото не е 3 пъти по голямо от най-ниското), а съотносителните мащаби дават възможност за по-голяма измеримост (например, класиране на 10 нива е 5 пъти по-голямо от класиране на 2). Описаните типове измерителни мащаби не са приложими за всяка компания без тяхното конкретизиране.

3. МОДЕЛ ЗА ОЦЕНКА НА КОРПОРАТИВНИЯ РИСК КАТО ЧАСТ ОТ ИВУС

Основни стъпки за извършване на оценка на риска

Извършването на оценка на риска изисква текущо и последователно прилагане на метод/подход, който е съобразен с организацията. Всяка проведена оценка на риска трябва да започне със създаването на обхват и план, имайки предвид целите, отговорностите, времето, както и входните и изходните изисквания. Отговорности в процеса на оценка на риска са възложени на пряко свързани служители, които могат да дадат смислен поглед върху съответните рискове. Източници на входни данни се определят въз основа на наличната информация (например, предварителни оценки,

загуба на данни, извлечените поуки). Изходната информация на процеса се планира въз основа на спецификациите в изискванията на спонсори и други заинтересовани страни (например, висш ръководен състав, на борда, регулатори, акционери или бизнес партньори).

След като определянето на обхвата и планирането са извършени, изпълнението на процеса на оценка на риска трябва да включва следните основни стъпки:

1. Идентифициране на процеси и активи, както и рискове;
2. Идентифициране на събитие;
3. Определение на критерии и изисквания спрямо оперативната дейност и нейните рискове;
4. Оценка на риска;
5. Реакция спрямо риска – Приемане на риск, Прехвърляне на риск, Третиране на риск.

Критерии за анализ на риска

Метриката за измерване на риска се базира на вероятност и въздействие, както е посочено в табл. 4.

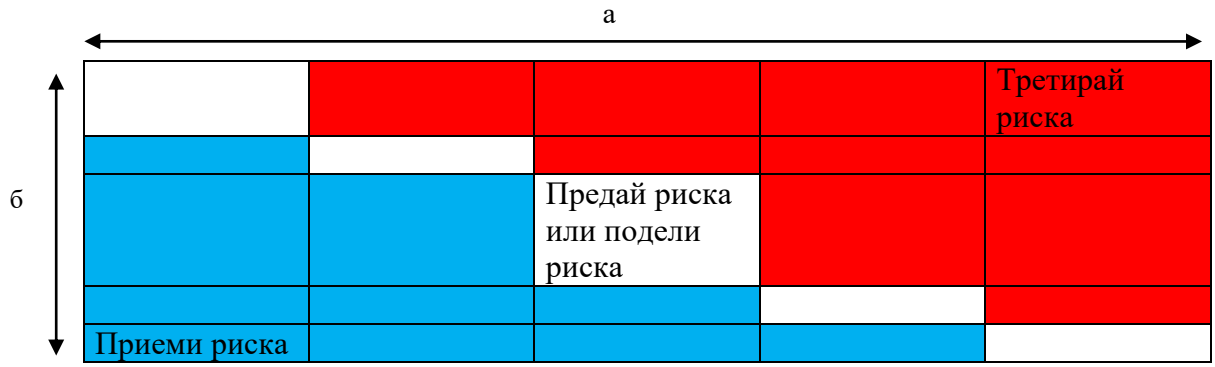
Табл. 4. Критерии за анализ на риска, спрямо вероятността и въздействието.

Вероятност	**Дефиниции**	**Описание**	**Пример**
1	Малко вероятно	Рискът се разглежда като малко вероятно да се случи в рамките на времевия хоризонт (например 1 година).	Мерки за физическа сигурност като например видео наблюдение, охрана, картова система са внедрени, но въпреки това има вероятност да има физически пробив.
2	Вероятно	Рискът е по-вероятно да се случи в рамките на времевия хоризонт.	Картовата система на компанията работи без съществено криптиране на картовата информация (права за достъп). Възможно е копиране на карта за достъп.
3	Предстоящо	Рискът се очаква да се случи в рамките на времевия хоризонт.	Физическата охрана не е обучена адекватно, което ще доведе до инцидент в сферата на физическата сигурност.
Въздействие	**Дефиниции**	**Описание**	**Пример**
1	Пренебрежимо	Рискът ще нанесе минимални щети на активи на организацията.	Отпадане на поддържаща некритична система. Оперативната дейност не е застрашена.
2	Умерен	Рискът ще нанесе умерени щети на активи на организацията.	Отпадане на оперативно важна поддържаща система. Оперативната дейност е застрашена, но все още е активна.

3	Критично	Рискът ще нанесе критични щети на активи на организацията.	Отпадане на оперативно важна критична за дейността система. Оперативната дейност е застрашена и отпада.

Измерването на риска спрямо определените критерии и параметри на реакция, са посочени в табл. 5.

Табл. 5. Модел за оценка на риска и управлението му.



Пояснение на табл.5:

а) Вероятност от малко вероятно до предстоящо събитие (както е посочено в табл. 3);

б) Въздействие от ниско до високо спрямо съответен актив на компанията (както е посочено в табл. 3).

4. ЗАКЛЮЧЕНИЕ

В настоящата работа са разгледани конкретни въпроси, свързани с анализ и оценка на риска, приложими в телекомуникационни структури. В тази връзка е дадена дефиниция и е направен анализ на процеса на „оценка на риска“. Предложен е модел за оценка на корпоративния риск като част от интегрирана вътрешна управленска система.

Развитието на разработката може да включва анализ на числови стойности и примери при различни компании.

ЛИТЕРАТУРНИ ИЗТОЧНИЦИ:

[1] ISO/IEC TR 18044:2004 Information technology - Security techniques - Information security incident management

[2] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control - Integrated Framework (23. Март 2011), Enterprise Risk Management — Integrated Framework (23. Март 2011), Guidance on Monitoring Internal Control Systems

[3] Tomov K. Development of an integrated internal management system (IICS) model and a efficiency measurement algorithm. Annual Proceedings of New Bulgarian University (Department of Telecommunications), 2014, vol. 1, pp., ISSN 2367-5039 (In Bulgarian: Разработка на модел на интегрирана вътрешна управленска система (ИВУС) и алгоритъм за оценка на оперативната ефективност).

[4] Strategic Risk Taking: A Framework for Risk Management, Aswath Damodaran, ASIN: B0055OD9Y0, 02.08.2007.

[5] Operational Risk Management: A Complete Guide to a Successful Operational Risk Framework, John Wiley, ISBN-10: 1118532457, 29.11.2013.

[6] Fraud Risk Assessment: Building a Fraud Audit Program, Leonard W. Vona, ASIN: B008O5GR64, 27.Май.2008.
[7] Risikomanagement - Sachversicherungen für private und gewerbliche Kunden, Markus O. Robold и Manfred Lange, ISBN-10: 3899527151, 18.12.2012
[8] Market Risk Analysis: 4 Volume, Carol Alexander, ISBN-10: 0470997990, 23.01.2009.
[9] Optimale Produktgestaltung: Erfolgsprognose mit Analytic Hierarchy Process und Conjoint-Analyse, Dieter K. Tscheulin, ISBN-10: 3409134468, 01.12.1992.
[10] Supply Chain Risk Management: Vulnerability and Resilience in Logistics, Donald Waters, ISBN-10: 0749463937, 03.10.2011.
[11] ISO/IEC 27004:2009 Information technology -- Security techniques -- Information security management – Measurement, от International Organization for Standardization (ISO) и International Electrotechnical Commission (IEC), публикувано в 2009 г.

За контакти:
Кристиан Томов, Департамент”Телекомуникации” на НБУ, ул. Монтевидео № 21, 2609, Тел.: 02 8110609, e-mail: kristiantomov@yahoo.com