St. Cyril and St. Methodius University of Veliko Tarnovo
Faculty of Economics

РОЛЯ НА ПОДХОДА „УПРАВЛЕНИЕ, РИСК И СЪОТВЕТСТВИЕ“ В ОРГАНИЗАЦИИТЕ

THE ROLE OF THE GOVERNANCE, RISK AND COMPLIANCE APPROACH IN ORGANIZATIONS

Даниела Йорданова
Daniela Yordanova

Великотърновски университет „Св. св. Кирил и Методий“
St. Cyril and St. Methodius University of Veliko Tarnovo

Abstract: Public and private sector organizations operate in a highly regulated environment. Part of the decisions of their managers are related to maintaining the activities within the requirements of compliance with the external regulatory framework, the regulations of the superior authorities, and the limitations imposed by legislation. The purpose of this report is to show the essence of the management, risk and compliance approach and its application possibilities, justifying the main principles on which it is based. In addition, basic risk management functions and steps are covered, and good practices for risk and compliance management (GRC) in organizations are presented in an international aspect and in Bulgaria.

Keywords: organizations; approach; risk; compliance; governance.

JEL: D81

ВЪВЕДЕНИЕ

Днес управлението на риска е водеща концепция в мениджмънта на организациите от публичния и частния сектор. Докато в частния сектор се прилагат принципите на корпоративното управление и корпоративния контрол, в организациите от публичния сектор се прилагат тези на доброто финансово управление и финансовия контрол съгласно Закона за публичните финанси (Public Finances Law). Подходът „Управление, риск и съответствие“ се отнася до стратегията за цялостно управление на организацията, като същевременно ефективно се управлява риска и отговор на нормативните изисквания. Човек трябва да е добре запознат с управленската рамка, да документира рисковете, които е вероятно да възникнат, и да гарантира, че организацията спазва изискванията на регулаторните органи. Това позволява на организациите да бъдат проактивни по отношение на бъдещи загуби и други рискове (Njoroge, 2020). Ръководителите на публични организации подложени на контрол за ефективното използване на публичните средства и по този начин те трябва да насърчават култура, при която да се действа в най-добрия интерес на гражданите. Затова е необходимо да се създадат механизми за управление, които да регулират поведението

им с цел постигане на максимална икономичност, ефикасност и ефективност при използване на предоставените им публични ресурси.

ИЗЛОЖЕНИЕ

Съществуват много дефиниции на риска като понятие. Това, което е заплаха за един мениджър, е възможност за друг. Обвързан с цялостната концепция за мениджмънта в организациите, рискът може да се възприеме като възможност за възникване на проблем от настъпването на потенциално събитие, което би затруднило дейността на организацията и би попречило за постигането на целите й (Cendrowski & Mair, 2009, p. 12). Рискът като понятие може за се определи като бъдещо събитие, носещо несигурност, което може да окаже влияние върху развитието на една организация в стратегически, операционен и финансов аспект (Harvey, 2008).

Според съществуващи в литературата обобщения на експерти в областта на управлението на риска, основните затруднения и предизвикателства, свързани с управлението на риска в организациите на съвременния етап включват: създаване на общ език или речник по отношение на риска; определяне на склонността на организацията да рискува; идентифициране и описване на рисковете в „списък на рисковете"; прилагане на методология за определяне на приоритетни рискове; обвързване на отговорността за всеки риск с конкретен служител (или група от служители); отчитане и сравняване на разходите и ползите от усилията за управление на риска; разработване на планове за действие за осигуряване на подходящо управление на риска; мониторинг на резултатите от предприеманите действия за смекчаване на риска. Въз основа на анализ на съществуващи теоретични постановки основният проблем при управлението на риска се състои в разбирането, че за всеки риск е необходим подход. (Stefanov&Dilkov, 2004, p. 40)

Актуалността на разглеждане на подхода „Управление, риск и съответствие" се поражда от факта, че днешните рискове са все по-взаимосвързани от всякога. Един риск – например проблем със здравето и безопасността може да се разпространи върху веригата за доставки, непрекъснатостта на бизнеса, бизнес взаимоотношенията, ИТ сигурността, производителността на работната сила и др., както за бизнес организациите, така и в публичния сектор. В същото време множество сили променят риска, включително: нарастващи темпове и обхват на съответствие с нормативните изисквания, изразяващи се в непрекъснато нарастващ и постоянно променящ се брой регулации, с които трябва да се съобразява дадена организация, ускоряване на дигитализацията на управлението на риска. Управлението на риска все повече се разглежда не само като тактическа функция, но и като ценна част от стратегията на организацията, включващи анализ и решения, базирани на данни (Governance, Risk, and Compliance:The Definitive Guide).

1. За подхода „Управление, риск и съответствие" (GRC – Governance, Risk and Compiance)

GRC е интегрираната колекция от възможности, които позволяват на организацията надеждно да постига цели, да се справя с несигурността и да действа почтено. Първото научно изследване е публикувано през 2007 г., но оригиналните идеи са създадени през 2003 г. от експерти на OCEG. Те официално дефинират подхода „Управление, риск и съответствие" като важен стандарт за интегриране на управлението, одита и изпълнението, риска, съответствието и етиката за надеждно постигане на целите на организацията. А това води до справяне с несигурността и почтено действие. (OCEG)Следва да се отбележи, че ефективното управление на риска и управлението на съответствието изисква информация, която е пълна, лесно достъпна и използваема, за да позволи бързо вземане на решения, вместо да го възпрепятства. За съжаление информацията в повечето организации се поддържа в различни системи или електронни таблици и се управлява от различни отдели (The Public Sector with Keylight, 2019). Оптималният начин за справяне с разрушителни инциденти, е спазване на разпоредбите, предназначени да ги предотвратят. Без интегриран поглед върху всички дейности, е почти невъзможно да се идентифицират проблеми и несъответствия. Защото когато нещата са изолирани, е по-вероятно да бъдат установени грешни или непродуктивни цели, да бъдат избрани неоптимални стратегии и ефективността да не е оп-

тимизирана. **Основните принципи** на подхода „Управление, риск и съответствие“ са: (Kirvan & Gillis, 2021)

• Управлението се отнася до етичното управление на организация от нейните лидери в съответствие с одобрените планове и стратегии.

• Управлението на риска се отнася до процеса на организацията за идентифициране, категоризиране, оценка и прилагане на стратегии за минимизиране на рисковете, които биха попречили на нейните операции, и за контролиране на рисковете, които подобряват операциите.

• Съответствието се отнася до нивото на придържане на една организация към стандартите, разпоредбите и най-добрите практики, определени от организацията и от съответните ръководни органи и закони.

Управлението, риска и съответствието са три ключови проблема, които оказват сериозно влияние върху цялостната дейност. Процесите на управление на дейностите, оценката и въздействието на рисковете, които съпътстват дейността им, както и необходимостта от въвеждане на ефективни програми за съответствие с изискванията, са водеща концепция в мениджмънта на публичния сектор. Въведени са като концепция от Интегрираната рамка за управление на риска в предприятеието „COSO“ и се обозначават като „GRC“ (Governance, Risk and Compiance). (ENTERPRISE Risk Management – Integrated Framework COSO, 2004).

2. Основни функции за управление на риска – практики в България

Позовавайки се на вижданията относно функциите на риск-мениджмънта, ще разгледаме основните функции на управлението на рисковете, конкретизирани към практиката на организациите от публичния сектор в България. Те са следните функции (Gabrovski & Iliev, 2004, p. 92-93):

– Превантивна функция. Тя е свързана с предпазване на материалите, финансовите и човешките ресурси на организацията от загуби, увреждания, лош мениджмънт. Стремежът на ръководството трябва да е насочен към превантивността с цел идентифициране и оценка на неблагоприятните събития, които биха довели неблагоприятни резултати.

– Ограничителна функция. Тази функция има рестриктивен характер. Тя е свързана с разработване на програми в организацията, които да ограничават ръководителите им от вземане на неправилни решения в области с наличие на висок риск.

– Разпределителна функция. Тази функция има съществено значение при определяне на правата и отговорностите на ръководителите и останалия персонал в организацията по отношение на участието им в процеса по управление на риска. Разпределянето на отговорностите е функция на управлението и се влияе от съществуващата организационна структура в организацията.

– Информационна функция. Тази функция произтича от факта, че от процеса на идентифициране, оценка, анализ, изготвяне на реакция и мониторинг на рисковете се натрупва изключително голяма като обем икономическа и статистическа информация.

Заедно тези функции представляват основа за създаване на подход за разработване процеси по управление на рисковете.

В българската практиката на организациите, законодателството е въвело, че техните ръководители носят отговорност за идентифицирането, оценката и управлението на рисковете, застрашаващи постигането на целите на организациите. (Law on Financial Management and Control in the Public Sector) Следователно изграждането, организацията, въвеждането и контролът на ефективното осъществяване на цялостния процес е ангажимент на ръководствата, както и участието на всички служители. При изграждане на процесите по управление на риска ръководителите на тези организации трябва да вземат под внимание следните няколко основни изисквания (Law on Financial Management and Control in the Public Sector):

– Да разработят и утвърдят стратегия за управление на риска, която да определя обхвата, методите и техниките за идентификация и оценка на рисковете, начините на документиране и докладване на резултатите, честотата и интензивността на наблюденията (мониторинга) на процеса по неговото управление и като бъде съответстваща на политиката и целите на организацията като цяло.

– Ключов фактор за въвеждане на успешен подход за управление на риска е разбирането за неговата важност и значение за добро финансово управление и вътрешния контрол.

– Служителите трябва да бъдат убедени и мотивирани да участват в процеса на управление на риска, осъзнавайки своята роля и отговорност. Участието на служителите при управление на рисковете трябва да е съобразено с техния административен капацитет и да им бъдат осигурени необходимите за това ресурси.

– Ръководството на организацията е необходимо да организира периодични прегледи на стратегията и процесите по управление на риска, с цел непрекъснато подобрение и съответствие с изискванията за адекватност.

Ръководейки се от тези изисквания, ръководителите на организациите от публичния сектор трябва да приложат конкретен подход за управление на рисковете. Такива подходи са дадени в Насоките на Министерството на финансите за въвеждане на управлението на рисковете в организациите от публичния сектор в България (Guidelines for implementing risk management in public sector organizations, 2008).

Ангажиментът на ръководството на организацията за управление на риска е функция на обхвата, желаната точност, риск-апетита на организацията и максимално допустимите разходи при идентифицирането, оценката и реакцията на рисковете (Cendrowski & Mair, 2009, p. 6).

3. Основни стъпки при управление на рисковете

Управлението на рисковете е ключова концепция в цялостния мениджмънт на организациите. Управлението на риска трябва да създава стойност, като подпомага подобряването на процесите, осигуряващи постигане на целите на организацията. Необходимо е да бъде неразделна част от организационните процеси, да бъде организирано по систематичен и структуриран начин при **спазване на основните стъпки в процеса на управление на риска**. Отправната точка е да се изгради пакет от цели, които произтичат най-вече от мисията, визията и стратегията на конкретната организация (Georgiev, 2013). Съгласно Насоки за въвеждане на управление на риска в организациите от публичния сектор в България, се включват следните стъпки (Guidelines for implementing risk management in public sector organizations, 2008):

Стъпка 1. Разработване на стратегия за управление на риска

Стратегията за управление на риска е ключов документ и изразява политиката и отношението на ръководството на организацията към цялостния процес по управление на риска в нея. Тя отразява основната концепция по избрания подход за управление на рисковете е неговата връзка с всички останали елементи на системите за управление и контрол в организацията.

Стъпка 2. Определяне областите на риск в организацията

Правилното разбиране за вида, характера и спецификите на всеки отделен риск, оказващ влияние върху постигане на целите на всяка една организация, започва с определяне на областите на риск в организацията. Областите на риск са важно изходно начало при разработването на всяка стратегия за управление на риска. Те са в зависимост от организацията на дейностите, спецификата на целите и задачите на организацията, практиките на управление, създадената среда (вътрешно нормативна база), изискванията за регулаторните рамки (външна нормативна база). Погледнато така, областите на риск са всички онези присъщи за организацията сфери на дейност, които покриват нейните цели. Определянето на областите на риск дава възможност да бъдат идентифицирани всички специфични и съществени рискове на детайлно ниво – дейности и операции.

Стъпка 3. Определяне на методиката и техниките за идентификация и оценка на риска

На основата на ангажимента за обхвата на Стратегията за управление на риска в определените области на риск ръководството на организацията трябва да определи методиката и техниките за идентификация и оценка на рисковете. В международната теория и практика по управление на рисковете са познати различни методи и техники за тяхната идентификация и оценка – от основани на експертна оценка, до статистически методи от теорията на вероятностите. Като *изход от идентификация на рисковете* е създаването на конкретна класификация на рисковете или т.нар. карта или портфолио на рисковете, специфицирани към всяка една, предварително определена

област на риск. От своя страна класификацията на рисковете е *вход за извършване на оценката на рисковете* в организациите. Портфолиото на рисковете е и основа за изработването на т.нар. „регистър на рисковете". Риск-регистърът е основен документ, свързан с цялостната документация на процеса за управление на рисковете в организациите.

Стъпка 4. Разработване на процедури за управление на риска

Процедурите представляват разписани правила или механизми, използвани за извършване на дейностите в съответствие с установените политики. Разписаните процедури в практиката обикновено са оформени в писмени наръчници с ясно разписани правила, отговорности, задължения и механизми за изпълнение на конкретни дейности чрез описана строга последователност от действия и операции. В процедурите за управление на риска се разписват необходимите действия и дейности, чрез които се осигурява разпределението на правата и отговорностите на ангажираните лица, протичането на процеса по управление на рисковете, видът и формата на документирането на резултатите от процеса.

Стъпка 5. Определяне на подход за реакция на риска

Изборът на подход зависи от характера на конкретния риск, възможността за неговата количествена оценка, риск-апетита на ръководството. Едни рискове могат да бъдат прехвърляни (риск от материални загуби, вследствие от природни бедствия - застраховане), други могат да бъдат споделени (риск от сериозна финансова инвестиция по конкретен проект – съвместен проект на две организации или публично-частно партньорство), трети да бъдат отказани (риск от финансови загуби), четвърти да бъдат контролирани (въвеждане на предварителен контрол на разходите с цел минимизиране на рисковете от незаконосъобразно или нецелесъобразно разходване на средства за издръжка на администрацията). Определянето на апетита към риск на организацията в стратегията за управление на рисковете е важен момент за създаване на адекватна реакция на рисковете. Риск-апетитът е количеството риск, което организацията и нейните ръководители са готови да приемат при преследването на конкретните цели. Това е склонността към поемане на риск при управление на дейностите.

Стъпка 6. Мониторинг на процеса по управление на рисковете

Основната цел на мониторинга е де предостави увереност на ръководството, че процесът по управление на риска е ефективен и ефикасен и е постигнат с минимални разходи. Мониторингът е основен ангажимент на ръководствата на организациите. Той може да се осъществява чрез *текущо наблюдение* и чрез *специални оценки*. За осъществяване на специалните оценки могат да се използват ресурсите на вътрешния одит в организацията.

Текущият мониторинг (рутинните дейности) е вграден в нормалните повтарящи се дейности в организацията. Много рутинни функции могат да бъдат характеризирани като дейности по мониторинг, например: прегледи на дейността от оперативния мениджмънт; преглед на обобщените доклади за изпълнение от висшето ръководство; засичане на наличността на активите и съпоставяне с отчетността (инвентаризации); оценка на квалификацията и уменията на служителите (атестиране) и т.н.

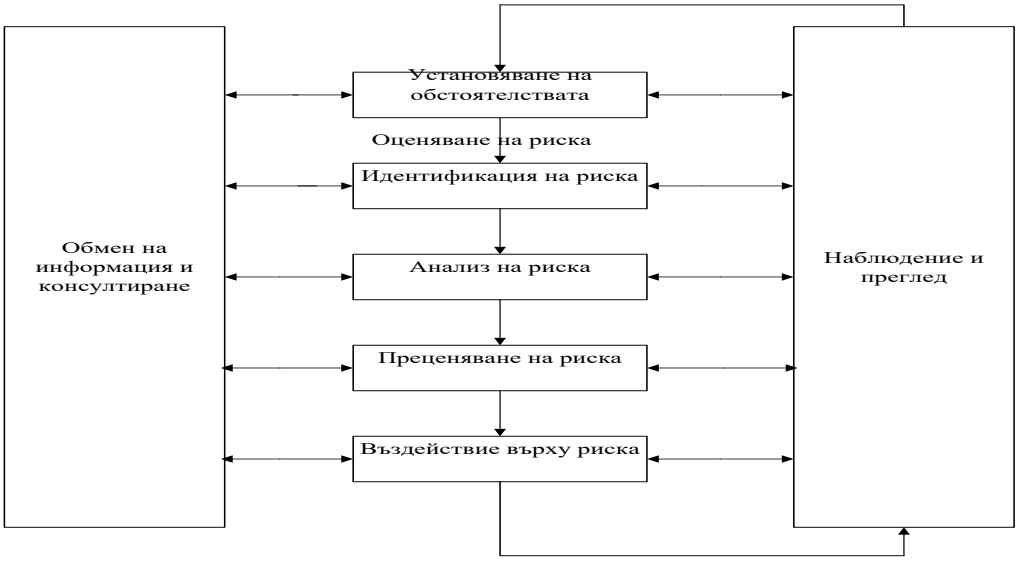
Специалните оценки са основен ангажимент на дейностите по вътрешен одит в организациите и зависят основно от оценката на риска и ефективността на текущия мониторинг. Вътрешният одит има за основна задача да извършва регулярни прегледи на ефективността и качеството на вътрешните контролни системи и тяхната адекватност на оценените рискове. Това изисква и преглед на процесите по управление на рисковете в организацията. За своите оценки вътрешният одит докладва на ръководството и предлага варианти за подобряване на системите за контрол и процесите по управление на рисковете.

4. Добри практики за управление на риска и съответствие (GRC) в организациите от публичния сектор

Водещи страни с ангажимент към управлението на риска в публичния сектор са предимно европейски държави, но Канада и Австралия също имат забележим и добре признат ангажимент към управлението на риска. Международно признат стандарт за управление на риска

е ISO31000:2009. Независимо от това, Австралия и Канада имат много полезен и изчерпателен опит за рисковете в публичния сектор. Австралийски стандарт (AS/NZS 4360:1995), по-късно препубликуван с някои нови версии, предлага подробно обяснение за риска в публичния сектор и стъпките, които трябва да се предприемат за ефективното му управление. Най-новата версия е тази от 2009 г., озаглавена „AS/NZS ISO 31000:2009 – Съвместен международен стандарт за управление на риска в Австралия и Нова Зеландия/Принципи и насоки“, която преустанови AS/NZS 4360:2004. Документът предлага подробни насоки за управление на риска (Standards Australia/ Standards New Zealand, 2009). През 2009 г. се въведе стандарта ISO за управление на риска. Чрез него управлението на риска стана стандартизирано в световен мащаб, тълкувайки риска като „ефект на несигурността върху целите“ (Gleim, 2004, p. 162). Стандартът ISO 31000:2009 съдържа изчерпателен набор от принципи и насоки за управление на риска. Предназначен е за широк кръг потребители, приложим в различни организации и сектори и дава препоръчителни насоки. Променящите се закони, регулаторни рамки, политики на държавата, а заедно с това и социално-икономическите отношения създават определена степен на неопределеност по отношение на решенията за реакция от страна на ръководствата в организациите (Ivanov, 2013, p. 46-47).

Основните предпоставки и причини за бързото развитие, теоретичното обогатяване на обекта и предмета и усъвършенстването на концепциите за риск-мениджмънта, са обществено-икономическите потребности, предизвикани от динамичните промени в системите като в глобален, така и в локален мащаб (Gabrovski & Iliev, 2004, p. 92-93). Степента и разнообразието от рискове, пред които са изправени държавните органи в ежедневната си дейност, са огромни и основната отговорност на тези органи е да уверят обществеността, че нито един текущ или потенциален риск няма да застраши възприеманата обществена стойност. Ръководителите на организациите носят отговорност за цялостния процес по управление на рисковете, както и за осигуряване на текущ мониторинг върху него и актуализиране при необходимост. След въвеждането на стандарта ISO през 2009 г., се предлага всеобхватен модел на процес за управление на риска, състоящ се от 7 стъпки, приложими в различни индустрии и сектори. (BDS ISO 31000) Те са представени на Фигура 1.



Фигура 1. Модел на процеса за управление на риска по ISO 31000: 2009
Източник: БДС ISO 31000 „Управление на риска. Принципи и указания

Представеният модел на процес за управление на риска, е ключов за придържане към принципите за добро финансово управление, а следователно и за спазване на принципите на подхода „Управление, риск и съответствие“.

Практиките показват, че използването на подхода „Управление, риск и съответствие“ гарантира установяването на правилните цели, въведени са правилните действия и контроли, за да се отговори на несигурността и да се действа почтено. Става дума за установяване на подход, който гарантира, че точните хора получават точната информация в точните моменти. Организациите, които интегрират подхода „Управление, риск и съответствие“ към процеси и технология във всички или много области, които преди са били изолирани, отчитат предимства като: (OCEG. What is GRC)

- намалени разходи;
- намалени излишни или дублиращи се дейности;
- намалено въздействие върху операциите;
- постигнато по-високо качество на информацията;
- постигната по-голяма способност за бързо и ефективно събиране на информация;
- постигната по-голяма способност за повтаряне на процесите по последователен начин.

Практиките за добро управление, управление на риска и съответствие са от съществено значение за укрепване на устойчивостта на бизнеса и доверието в организациите.

ЗАКЛЮЧЕНИЕ

От така направения преглед на подхода „Управление, риск и съответствие“ и възможността за неговото имплементиране към управлението в организациите от публичния сектор могат да се направят следните обобщаващи изводи:

1) Организациите от публичния сектор са изправени пред различни видове рискове, които могат да повлияят върху постигането на техните цели. Пред ръководителите им стои проблемът, как да се определят значимите рискове, как да бъде оценена вероятността за настъпването им и степента на тяхното влияние и каква реакция да бъде предприета срещу тях, за да се ограничат те до едно приемливо равнище.

2) Рискът от съответствие е свързан с изискванията за съответствие, които се управляват от новата технология и обхвата на данните, създавани от организацията. С всяка нова технология често има нови изисквания или правила, които също трябва да бъдат приложени, или се рискува неспазване на регулаторните изисквания.

3) Успешното внедряване на подхода „Управление, риск и съответствие”, заедно с подобрения в риск мениджмънта и вътрешния одит, ще има положително въздействие върху цялостното представяне и постигането на целите. Разработването на подхода е особено важен за големи организации, които имат обширни изисквания за управление на риска и съответствие, и където програмите за изпълнение на тези изисквания често се припокриват.

4) Прилагането на подхода „Управление, риск и съответствие“ ще спомогне организациите да осъзнаят, че координирането на хората, процесите и технологиите, които използват за управление, от една страна и риск и съответствие от друга, може да бъде от полезен чрез: гарантиране, че техните организации действат етично. Това би помогнало да постигнат целите си чрез намаляване на неефективността и грешки в комуникацията.

5) Практиките показват, че използването на подхода „Управление, риск и съответствие“ гарантира установяването на правилните цели, въведени са правилните действия и контроли, за да се отговори на несигурността и да се действа почтено. А това ще гарантира, че точните хора получават точната информация в точните моменти.

REFERENCES

BDS ISO 31000 „Risk management. Principles and guidelines. (in Bulgarian)

Cendrowski, H. and W. C. Mair. 2009. Enterprise Risk Management and COSO, a Guide for Directors, Executives and Practitioners, John Wiley & Sons, p. 6-12.

Gabrovski, R., B. Iliev. 2004. Corporate risk management, AI „Tsenov“, Svishtov, pp. 92-93. (in Bulgarian)

ENTERPRISE Risk Management – Integrated Framework COSO, 2004. Committee of Sponsoring Organizations of the Tread way Committee.

Georgiev, I. 2013. Risk management in public sector organizations, AI Tsenov, SA "D. A. Tsenov", Svishtov. (in Bulgarian)

Gleim, I.N. 2004. CIA REVIEW, Part I, Internal Audit Role in Governance, Risk and Control, 11 edition, Gleim Publications, Inc., p. 162.

Governance, Risk, and Compliance:The Definitive Guide; Available at: https://riskonnect.com/resources/grc-guide/

Guidelines for implementing risk management in public sector organizations, Ministry of Finance, Sofia, 2008. (in Bulgarian)

Harvey, J. 2008. Introduction to managing risk. Chartered Institute of Management Accountants, Available at: http://www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_intro_to_managing_rist.apr07.pdf

Ivanov, G. 2013. Risk management in public sector organizations of the Republic of Bulgaria. Academic publishing house „DA Tsenov", Svishtov, pp. 46-47. (in Bulgarian)

Kirvan, P., A. Gillis. 2021. Governance, risk management and compliance (GRC); Available at: https://www.techtarget.com/searchsecurity/definition/governance-risk-management-and-compliance-GRC

Law on Financial Management and Control in the Public Sector, promulgated SG No. 21 of March 10, 2006, amended SG No. 15 of February 15, 2013. (in Bulgarian)

Methodological guidelines on the elements of financial management and control, Ministry of Finance, Sofia, 2006. (in Bulgarian)

Njoroge, G. 2020. Managing your organizations' Governance, Risk, and Compliance (GRC) activities, Available at: https://www.linkedin.com/pulse/managing-your-organizations-governance-risk-grc-george-njoroge-/

OCEG. What is GRC, Available at: https://go.oceg.org/what-is-grc/?_ga=2.55988651.1216290643.1663924808-1503375752.1663924808#action

Public Finances Law, OBN. - SG, BR. 15 OF 2013, in force from 01.01.2014. (in Bulgarian)

Standards Australia/Standards New Zealand, 2009

Stefanov, St., Cv. Dilkov. 2004. Risk Management. Academic ed. Priced. Svishtov, p. 40. (in Bulgarian)

The Public Sector with Keylight, 2019; Available at:https://www.navex.com/en-us/resources/datasheets/compliance-risk-management-public-sector/

За контакти:
Даниела Йорданова, доцент, доктор
Служебен адрес: гр. Велико Търново, 5000, ул. „Арх. Г. Козаров" №1
Великотърновски университет „Св. св. Кирил и Методий"
Стопански факултет
Катедра „Стопанско управление"
Ел. поща: daniela.yordanova@ts.uni-vt.bg