DOI: https://doi.org/10.37075/ISA.2020.2.03

Анализ и оценка на операционните рискове

Антон Герунов*

Резюме: Статията разглежда основни моменти от управлението на операционните рискове. Очертават се основни типове операционни рискове и се прави преглед на техните специфични особености спрямо други видове стопански риск. Представя се общ модел за количественото им управление, както и набор от добри организационни практики, използвани в този процес. На база на обстоен преглед на актуалната научна литература, извеждаме четири нови тенденции в тази област на изследвания: засилено внимание към конкретни индустрии и казуси, разширен фокус върху информационните технологии, навлизане на нови авангардни статистически алгоритми и преминаване към интегрирана представа за общата рискова експозиция на съвременната организация. Резултатите могат да се използват както като отправна точка за нови научни изследвания в областта, така и да бъдат в помощ на практическия управленски процес.

Ключови думи: операционен риск, управление, методология за управление.

JEL: D81, M10.

Въведение

Стопанският риск е неразделна част от икономическата реалност. Той представлява несигурни събития, които могат да имат ефект върху общото състояние на даден индивид или организация. Поради регулативни причини, традиционно финансовият сектор е естествена лаборатория за анализ и апробиране на различните методи и подходи за управление на риска и то най-често финансовия такъв. От друга страна, технологичните и икономически развития поставят на преден план общото холистично управление на всички видове организационни рискове, като операционният такъв се откроява като особено важен. Макар общата дефиниция за стопански риск да е относително устойчива и широко възприета, то определенията за различните типове риск варират в значителна степен. Фокусирайки се върху операционния риск, следва да отчетем, че той се дефинира по различен начин от различните автори.

Leone et al. (2018) правят подробен преглед на алтернативните дефиниции на понятието операционен риск, като стъпват върху практиката в банковата сфера, където операционен риск се дефинира като рискът от загуба, произтичащ от неадекватни вътрешни процеси, човешки грешки или неуспешно функциониране на определени системи. Подобна е и дефиницията на Jorion (2000). Към тази дефиниция Банката за международни разплащания добавя и риска, произтичащ от външни събития (вж. BIS, 2001). В практиката се налага много по-широко разбиране за операционен риск, като Deutsche Bank (2005) го дефинира като потенциала за реализиране на загуби, произтичащи от действията на служителите, договорните

* Антон Герунов е доктор по икономика, доцент в Стопанския факултет на Софийски университет „Св. Климент Охридски“.

отношения и документацията, наличните технологични решения, нефункциониране на инфраструктурата, инциденти, външни влияния и отношения с клиентите. Удачно е да се използва именно разширената дефиниция на операционния риск, тъй като тя позволява да се обхване пълноценно множеството от рискови ситуации в рамките на ежедневните дейности на организацията, които подлежат на автоматизация от електронни системи. В този смисъл се придържаме към дефиницията за операционен риск на King (2000), който го определя като „мярка за връзката между бизнес дейностите (процесите) на организацията и нейните резултати", като отчитаме важността на основните четири групи рискови фактори: хората, процесите, системите, външните събития (Chernobai et al., 2012). Използването на тази дефиниция позволява и по-пълната концептуализация на операционния риск като хоризонтален риск за всички дейности на съвременната организация (Leone et al., 2018).

Типове операционни рискове

В рамките на общия рисков контекст на организацията, операционните рискове са ключов елемент от общата експозиция към потенциални загуби (или печалби). Едно от значителните предизвикателства при тяхното управление е широкият спектър от потенциални източници на такива рискове, като за аналитична яснота си струва да очертаем основните типове операционни рискове. Ще използваме две основни типологии (Jarrow, 2008 и Embrechts et al., 2003), като подчертаваме, че те са до голяма степен представителни за общия научен консенсус в областта.

Jarrow (2008) разделя операционните рискове на две основни групи – дискреционни (които зависят от вътрешните действия и решения на организацията) и системни (които зависят от външни за организацията фактори). Сред дискреционните рискове попадат произтичащите от действията на служители и от условията за безопасен труд рискове, както и вътрешните измами. Сред системните рискове попадат: външните измами, рисковете, свързани с клиенти продукти и бизнес практики, както и потенциалното разрушаване на активи. Освен това, тук се включват и събития, които прекратяват дейността на бизнеса, водят до преустановено функциониране на системите, както и рисковете, свързани с изпълнението и управлението на организационните бизнес процеси.

Стъпвайки върху класификацията на Crouhy et al. (2001), Embrechts et al. (2003) съставят сравнително подробна класификация на основните операционни рискове в дадена организация, като ги делят на три основни групи – рискове, свързани с хората, с процесите и с технологиите. Допълнително, тези рискове могат да бъдат отчетени като еднократни или повтарящи се, което дава и първоначална идея за рисковата експозиция на дадена организация. Те са както следва:

- **Човешки рискове** – те са обусловени от основните отрицателни събития, които могат да възникват поради човешкия фактор в дейността на дадена организация. Основните сред тях са измамите (вътрешни и външни), както и грешките, допуснати поради некомпетентност или неподготвеност на служителите.
- **Процесни рискове** – тук се включват всички потенциални негативни последствия от проблеми в бизнес процесите, като основните групи са моделните рискове, транзакционните рискове и рисковете на процесния контрол. Моделните рискове са предизвикани от погрешен модел или методология за извършване на дадено действие, както и разминавания между оценките на модела и реалните стопански факти. Транзакционните рискове са предизвикани от грешки при изпълнението на транзакцията, от сложността на продукта, от неправилно отчитане, от погрешен сетълмент или

приключване, както и в резултат от проблеми с документацията или договорите. Рисковете на процесния контрол включват потенциални усложнения при надвишаване на определени лимити, при обработка на големи обеми и рискове за сигурността.

- **Технологични рискове** – произтичат от разширяващата се употреба на информационни и комуникационни технологии (ИКТ) в съвременните организации и отчитат разширяващата се експозиция на операциите към автоматизирани системи. Основните източници на такива рискове са прекъсвания на работата на системи и телекомуникационна инфраструктура, грешки при програмирането, информационни рискове.

Някои от изброените рискове са с повторяем характер, което предполага постоянно управление, докато други са еднократни – след тяхната реализация те напускат регистъра на риска. Макар това разграничение да е теоретично интуитивно, на практика рисковите събития невинаги могат да бъдат еднозначно определени, затова е по-удачно да отчетем преобладаващия характер на събитията – еднократни или периодични. Така представената класификация е до голяма степен представителна за използваните в литературата и също така е използвана в регулативната практика (Chernobai et al., 2007).

Особености на операционния риск

Операционният риск има редица особености, които правят неговото идентифициране и управление значително предизвикателство в практически, а и в изследователски план (Moosa et al., 2007). Преди всичко отбелязваме, че операционният риск е хоризонтален такъв и се отнася до всички дейности или бизнес процеси в дадена организация. Той може да се появи във всеки един отдел и в резултат на действията (или бездействията) на всеки служител, клиент, информационна система или дори инфраструктурен компонент. В този смисъл, операционният риск е значителен по обхват и сравнително по-труден за дефиниране и идентифициране. Съществуват и трудности при отграничаването на операционния риск от други типове рискове (пр. бизнес, стратегически и репутационен), което налага внимателен подход при изследването му. От друга страна, в практически план организациите имат нужда от инструменти за управление на реално съществуващи и често нарастващи рискове, което предполага по-голям фокус на изследователските усилия върху анализ, прототипизиране и разработване на решения, и по-малък – върху извеждане на синтетични таксономии.

Второ, поради хоризонталния му характер, в организациите рядко има едно-единствено отговорно лице или дори структурна единица, която да бъде процесен собственик на пълния процес по управление. Това на практика означава, че операционният риск следва да се управлява от висшия мениджмънт с хоризонтален поглед върху цялата организация и нейните нужди. От изследователска гледна точка е важно операционният риск да се изследва в общия организационен контекст, като вероятно е удачно да се избегне излишното фокусиране върху дефиниционни въпроси и вместо това да се извеждат общи хоризонтални методи за изследване на този тип рискове. Като първа стъпка това могат да бъдат методи, приложими за различни индустрии, ситуации и типове организации, а на следваща стъпка – те да се адаптират за специфични нужди.

Трето, струва си да отбележим, че операционният риск често се възприема като чист риск (пр. Leone et al., 2018), тъй като се твърди, че той се предизвиква от отрицателни събития в рамките на обичайната дейност на организацията, които могат да доведат единствено до загуби. Авторът на

настоящата статия не споделя това мнение, тъй като операционният риск е изначално свързан с бизнес процесите и тяхното функциониране. В този смисъл, управлението на операционния риск неизбежно би довело и до оптимизация на бизнес процесите, което генерира по-висока продуктивност, повишена мотивация на служителите и подобрена репутация на организацията. Всички тези фактори водят и до подобрени финансови резултати. Поради тази причина настоящата работа разглежда операционния риск като спекулативен риск.

Четвърто, неизбежно е да се съгласим с Power (2005), който говори за т.нар. "експлозия на операционния риск" – фактът, че през последните 10-15 години се забелязва все по-засилен интерес към изследването и управлението на операционния риск както в научните среди, така и в стопанската практика. Това е обусловено от редица фактори, като особено важно е, че съвременната организация има все по-голяма експозиция към операционен риск поради дигиталната трансформация на нейните бизнес процеси и преструктуриране на дейностите ѝ в новата конкурентна бизнес среда (Leone et al., 2018).

По-специално отбелязваме следните важни фактори за увеличената рискова експозиция (ibid.):

- Разширена употреба на информационни системи, които трансформират риска от ръчни грешки в риск от проблеми на цялата ИТ система;
- Увеличено използване на дигитално банкиране и електронни плащания, увеличаващи риска от вътрешни и външни измами;
- Засилени процеси на сливания и придобивания, които водят до нужда от преструктуриране на организациите и тяхната интеграция от гледна точка на функции, процеси и системи;
- Увеличената свързаност между дейностите от различни бизнес направления с цел извличане на синергии от съвместната работа;
- Ръст на изнесените бизнес дейности извън организация (т.нар. „аутсорсинг"), който създава несъществуващи досега процеси и рискове;
- Увеличена вероятност за кибер-атаки, както и подобрено ресурсно обезпечаване на потенциалните атакуващи.

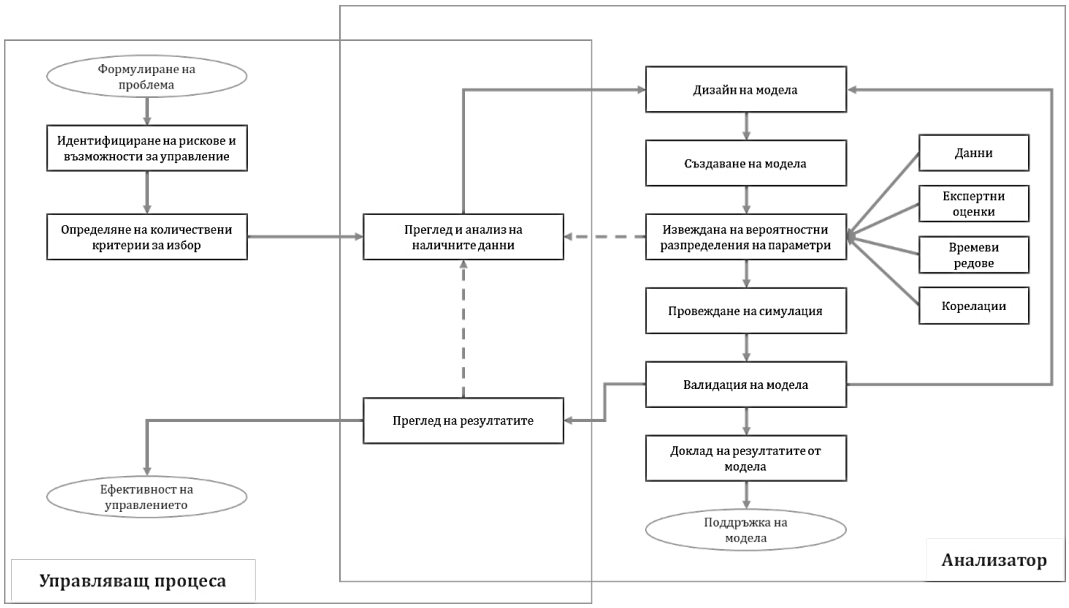
Обобщавайки, растящата сложност на икономическите транзакции, структурните промени в глобалната икономика и навлизането и все по-пълното използване на информационните и комуникационни технологии водят не само до възможност за повишена производителност и приходи, но и носят със себе си чувствителен ръст на операционния риск (Chernobai et al., 2018). Вероятно това е тенденция, която ще се ускорява през следващите години.

Процес на управление на операционния риск

С цел по-доброто разбиране на процесите за управлението на рисковете от гледна точка на тяхната автоматизация е удачно да се разгледат и разширените версии на съществуващите методологии. Vose (2008) представя детайлна методология за количествено управление на рисковете, като си струва да отбележим, че при нея са изрично очертани двете ключови роли на участващите в процеса:

- **Анализатор** – експерт, който моделира и оценява рисковете, като изгражда формален модел, произвеждащ резултати в услуга на формалната управлние;
- **Управляващ процеса** – най-често мениджър или група мениджъри, отговорни за управлението на рисковата експозиция.

Хронологично процесът на управление започва, като управляващият процеса формулира организационните проблеми и контекст и извежда списък от потенциалните рискове и възможностите за тяхното управление. Това може да бъде направено както от определен



Фигура 1. *Разширен процес за количествено управление на рисковете*

Източник: *Vose, 2008*

индивид, така и от групи ръководители и експерти, в зависимост от нуждите и практиките в съответната организация. Като важен момент тук отчитаме необходимостта от избор на количествени критерии за избор на подходящи модели, подходи и стратегии за управлението на риска. Всичко дотук може да се разглежда като входни данни за последващия аналитичен процес.

Аналитичният процес се състои от следните основни стъпки (Vose, 2008, с. 5), които обичайно се извършват от експерт или екип от експерти по управлението на рисковете (вж. ibid., с. 23-26, както и Kroenke et al., 2012; Larose et al., 2014; Lu, 2018):

- **Преглед и анализ на наличните данни** – първата стъпка е преглед и анализ на наличните данни. Това най-често включва описателен (дескриптивен) анализ, както и извеждане на връзките между различните променливи, които имат отношение към изграждане на общия модел на риск. Връзките могат да бъдат проследени както визуално (пр. чрез топлинна карта), така и аналитично (пр. чрез корелационна матрица).
- **Дизайн на модела** – като следваща стъпка експертите следва да изградят обща архитектура и структура на модела, който ще бъде използван за управление на риска. Тук е удачно да се избере както типът модел (ниво на формалност, използване на емпирични данни, симулация), така и конкретните алгоритми, които ще се използват (пр. корелационен или регресионен анализ, методи за машинно самообучение, алгоритми за оптимизация и други).
- **Създаване на модела** – тази стъпка включва изграждането на модела, като количествените модели често се изграждат и впоследствие изпълняват в конкретна софтуерна среда. На тази стъпка се осъществяват избраните в предишната такава подходи, като се прилагат различните подходящи алгоритми.
- **Извеждане на вероятностни разпреде-**

ления на параметри – след създаването на модела се оценяват параметрите, включени в него. При използване на подхода за оценка на параметри на база на предишни данни, тези параметри се изчисляват и се определя тяхното ниво на несигурност (най-често под формата на доверителен интервал). Извън оценката на основни характеристики на променливите понякога се налага да се изведе и тяхното статистическо разпределение, обобщено във функция на разпределение или плътност на вероятностите.

- **Провеждане на симулации** – използвайки изчислените оценки и изведените вероятностни разпределения на ключовите променливи, анализаторът може да направи симулации (пр. по метода Монте Карло), с които да отчете очакваните разпределения на резултатите, както и да оцени необходимите процентили на очакваните реализации на риска за нуждите на управлението му. На този етап може да се направи и сценариен анализ, който да покаже чувствителността на резултатите към промяна на някои или всички включени в него параметри. Подобен подход позволява да се количествени моделната несигурност, която…
- **Валидация на модела** – след изграждането на количествения модел, той следва да се валидира, като тази валидация може да бъде при сравнение с други модели (пр. на базата на информационен критерий, точност, обяснителна сила и др.) или на база на експертна оценка на получените резултати. Резултатите от валидирания модел могат да бъдат използвани на последващи стъпки от управленския процес.
- **Преглед на резултатите** – на тази стъпка се обсъждат получените от модела резултати и тяхната полза и приложение в рамките на общия процес. При този преглед участват както анализаторите, така и ръководителите на процеса и от организационна гледна точка това е момент не само на одобрение на получените резултати, но и на комуникация и изглаждане на потенциални различия.
- **Доклад на резултатите от модела** – след постигане на общо разбиране относно получените резултати от моделирането, те се оформят и се представят в подходящ формат в съответен доклад. Целта е визуализациите и аналитичното представяне да подпомогнат в максимална степен управленския процес.
- **Поддръжка на модела** – последната важна стъпка от аналитичния процес е поддръжката на модела, която включва както актуализация на данните и оценките на използваните параметри, така и техническата му поддръжка. Последното е особено в сила когато се ползват значителни по размер модели, изискващи комплексна изчислителна инфраструктура.

След приключването на аналитичната работа се избират стратегии за управлението на рисковете, предприемат се действия за целта и този процес формално се контролира. Всички тези дейности обичайно се извършват от мениджмънта на организацията и са интензивно от гледна точка на използваната информация и познание. Отбелязваме, че представеният от Vose (2008) подход в неговата аналитична част е сравнително широко разпространен за изграждане на формални математически и статистически модели, които са приложими не само към управлението на рисковете, но и към широк набор от други икономически дейности. Аналитичният подход е близък до този, препоръчван в литературата за съхранение, обработка и анализ на данни (Kroenke et al., 2012; Connolly & Begg, 2005; Cabena et al., 1997; Larose et al., 2014) и може да се каже, че отразява настоящия научен консенсус за аналитичен подход при работа с количествени данни. Нещо повече, този подход е залегнал и в практиката, като е отразен в широко използвания индустриален стандарт за изграждане на аналитични решения CRISP-DM, както и в други

сходни индустриални стандарти (Chapman et al., 2000; Azevedo et al., 2008; Daderman & Rosander, 2018; Lu, 2018).

Практики при управлението на операционния риск

Като допълнение към хоризонталните методологии за управление на риска подчертаваме и специфичните подходи и добри практики, които са свързани конкретно с операционния такъв. Чисто хронологично, операционният риск започва да бъде основен фокус на организациите на по-късен етап спрямо финансовите рискове, но регулаторни развития и по-специално необходимостта от провизиране на капитал за покриване на рискови събития с операционен характер (BCBS, 2006) водят до активното развитие на подходи и практики за управлението му. В своята работа Crouhy et al. (2006) очертават следния набор от важни моменти в управленския процес:

- **Политики** – първият елемент на управлението е създаването на подробни и добре дефинирани политики за операционния риск. В тях се включват както общите цели на организацията, ограниченията при нейната оперативна дейност, дефиниция на толерантността за поемане на риска, така и набор от стандартни оперативни процедури за изпълнение на различните бизнес дейности в организацията. Наборът от политики следва да определи рамката на процеса по управление на операционния риск и като цяло е добра практика при формализирането на всички управленски процеси (вж. пр. Hoyle, 2017).
- **Идентификация на риска** – тук целта е да се изгради единна терминология на процесите и обектите, както и единни наименования на типовете операционни рискове и съставляващите ги събития. Удачно е тези наименования да бъдат вписани в речник или справочен документ, който е широко достъпен за всички участващи в управленския процес.
- **Бизнес процеси** – този елемент включва извеждането и описанието на всички бизнес процеси, които организацията извършва за постигане на нейните цели. Често това се прави в диаграматична форма, като се използва формален език за моделиране. В практиката се налагат стандарти като UML (Ajina et al., 2018) и BPMN (Kopp et al., 2018), но от изследователска гледна точка няма голямо значение каква точно абстракция се използва при описанието на процесите. Извеждането на бизнес процесите позволява да се анализират конкретните оперативни дейности и да се изведат потенциалните операционни рискове, произтичащи от тях. Тези рискове се записват в Регистър на операционните рискове, който може да е част и от общия Регистър на рисковете на дадената организация.
- **Методология за измерване** – този елемент определя методологията за измерване на операционните рискове, дефинират се индикатори за рисковете и се определят начини за информационното им обезпечаване, като се определя и обхватът на всички данни, които ще се използват в процеса на управление на операционните рискове. В почти всички случаи се използват исторически данни за минали загуби, експертни оценки, симулационен анализ или комбинация от всички тях.
- **Управление на рисковата експозиция** – тук се вземат решенията за адекватно управление на идентифицираните и оценени операционни рискове. Препоръчително е да се осъществи анализ на ползите и разходите, който, заедно със стратегическите цели и рисковата толерантност на организацията, формира конкретните управленски подходи и стратегии за справяне с риска.
- **Докладване** – допълнителен важен елемент от процеса е определянето на това кои индикатори и мерки за риска

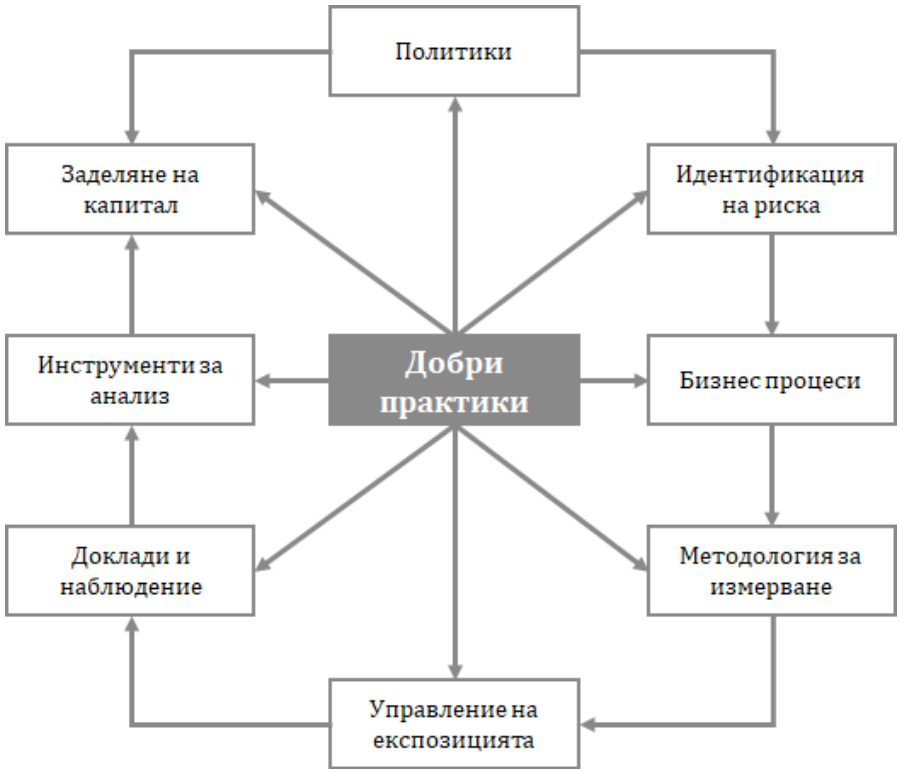
следва да се докладват в рамките на организацията за нейните бизнес нужди, както и кои метрики се докладват извън организацията за регулаторни цели, за нуждите на връзките с инвеститори, клиенти, партньори или като част от общата комуникационна стратегия. Важен момент тук е изграждането на подходяща организационна инфраструктура, която да обезпечи подготвянето и разпространението на определената информация за риска до всички заинтересовани страни. Тази инфраструктура може да бъде комбинация от…

- **Инструменти за анализ на риска** – като седми важен елемент можем да отчетем и разработването на конкретни инструменти за анализ и управление на риска, както и практики и стандартни за въвеждането им в продуктивен режим. Тези инструменти създават база данни с информация за операционните рискове в рамките на организацията и нейната референтна индустрия, подходи за изчисляване на метриките за рискова експозиция, добре дефинирани модели и сценарийни анализи, както и бази от познание за основните двигатели на операционния риск. Въз основа на тези инструменти може да се изчислят размерът и вероятността на операционния риск и съответните коефициенти, които го описват, като напр. операционната стойност под риск (Hartini et al., 2018).
- **Заделяне (провизия) на капитал** – последният важен елемент на добрите практики е, на базата на изведената операционна стойност под риск (т.е. очакваната операционна загуба при определен доверителен интервал), да се заделят финансови средства, които да покрият остатъчните очаквани загуби след прилагане на всички мерки за управление на риска. По същество това е икономически буфер, който остойностява несигурността, при която организацията оперира, и й позволява да осъществява безпроблемно дейностите си при реализиране на едно или повече рискови събития.

Отбелязваме, че подходът на Crouhy et al. (2006) е подчертано количествен, като голяма част от мерките и добрите практики допускат наличието на значителен по обем данни и аналитичен капацитет на организацията. В този смисъл, отчитаме тези добри практики като неподходящи за малки организации с ограничени инфраструктурни, информационни и аналитични възможности. От друга страна, високото ниво на структурираност, формалност и последователност на практиките за управление на операционния риск тук позволява алгоритмизирането на процеса и неговата последваща автоматизация с помощта на информационни системи.

Прави впечатление, че в българската научна литература практиките за управление на операционния риск са, в огромната си част, взети от банковата сфера, като в този случай регулативните изисквания поставят значителен отпечатък както върху фокуса на научните изследвания, така и върху научно-приложните аспекти на този процес (Стефанова, 2013; Димитрова, 2008; Милинов, 2010; Миланова, 2012; Минасян, 2012; Видолова & Георгиев, 2013; Анастасовки, 2018). Някои от тези разработки (ibid.) са по-скоро описателни, докато други имат и критичен характер. По-специално, Миланова (2019) отбелязва, че в контекста на регулативните изисквания операционните рискове са подценени, и очертава реформите на начините на измерване и управление на операционните рискове, предложени за потенциална нова версия на Базелските споразумения (BCBS, 2017).

Някои автори (Божинов, 2016) разглеждат някои от операционните рискове през призмата на рисковете за информационната сигурност в организацията. Подобен подход е изключително актуален и с нарастващо значение, тъй като цифровата трансформация на съвременните организа-



Фигура 2. *Елементи от процеса на управление на операционния риск*

Източник: *Crouhy et al., 2006, с. 328*

ции неизбежно ще доведе до дигитализиране на огромна част от бизнес процесите и дейностите и по този начин операционните рискове ще бъдат изключително свързани с дейността не на хора, а на автоматизирани системи. Като допълнителна тенденция Вълканов (2018) отбелязва нарастващата важност на операционните рискове на национално и международно ниво като функция на увеличаващата се комплексност на вътрешната и външната среда на организацията. Нещо повече, той (ibid.) подчертава и тенденцията към увеличено „грануларане“ (разбиване на всеки по-малки групи) при управлението на операционните рискове. Вълканов (2018) очертава и невъзможността на съвременната организация да се справи с рисковете, използвайки наличния традиционен инструментариум, и по този начин обосновава нужди от нетрадиционни и новаторски подходи.

Като допълнителен фактор за управлението на рисковете и направление на научните изследвания се очертават и организационните измерения, и по-специално – рисковата култура на организациите. Джарапов (2018) провежда подробно изследване на 304 респондента от девет банки с дял от 66,2% от всички активи в банковата сфера в България към 2016 г. и обосновава различия в рисковата култура, които впоследствие се отразяват и на практиките за управлението на рисковете. Тук подчертаваме, че подобна тенденция е неоднозначна, тъй като тя от една страна генерира възможност за иновация, а от друга може да доведе до устойчивост на някои неефективни практики.

Нови тенденции при управлението на операционните рискове

От гледна точка на новите научни изследвания в областта се наблюдава както прецизиране на настоящите методи и подходи (Embrechts et al., 2018; Leone & Porretta, 2018; Pena et al, 2018), така и постепенно навлизане на авангардни инструменти и новаторски подходи. Като основни нови тенденции отчитаме следните:

- Засилен фокус върху конкретни индустрии и специфични ситуации на управление на операционния риск;
- Задълбочаване на изследванията във връзка с риска и навлизането на информационните и комуникационни технологии;
- Навлизане на нови и авангардни методи за оценка на операционния риск и вземане на адекватни управленски решения в условия на несигурност;
- Постигане на интегрирана представа за общата рискова експозиция на организацията и намален фокус върху синтетичното разделяне на определените рискови групи.

Първо, струва си да отбележим тенденцията към приложението на методи и подходи за управление на операционния риск към конкретни индустрии, ситуации и организация. Yingqi et al. (2018), например, фокусират вниманието си върху операционните рискове в логистичния сектор и обосновават важността не само на вътрешните фирмени фактори, но и на общата макроикономическа среда, като изследват пет големи логистични компании. Rezapour et al. (2018) фокусират вниманието си върху управлението на мрежата от доставки, като отчитат два основни източника на риск – промяна в структурата (топологията) на мрежата, както и колебания в работата на участващите организации. Bandaly et al. (2018) също разработват интегриран модел за оценка на риска в контекста на управлението на веригата на доставките. Xu et al. (2019) се фокусират върху логистичните операции на компаниите за електронна търговия. Yang et al. (2019) разглеждат операционните рискове в контекста на газовата и нефтопреработвателна индустрия. Akgün (2018) разглежда и изследва операционните рискове в производството и показва методи за тяхното рационално управление. Cipriano (2018) също изследва операционните рискове в производството, като се фокусира върху събиране на вземанията. Основният резултат тук е отново, че върху операционния риск влияят както вътрешни фактори, така и външни макроикономически такива (инфлация и бета коефициент на компанията).

Chernobai et al. (2018) се фокусират върху финансовия сектор, като свързват общото ниво на комплексност на вътрешната и външната среда в банките с чувствителен ръст на операционния риск, с който те се сблъскват. Markou & Corsten (2018) изследват по-задълбочено управлението на финансовите и операционните рискове в златодобивната индустрия и представят доказателства не просто за ползата от двете дейности, но и за потенциалната допълняемост между тях. Khan et al. (2018) се фокусират върху изследването на операционните рискове при морското корабоплаване и по-специално – рискът от сблъсък между кораб и плуващи парчета лед, като за целта използват бейсови методи. Heaton et al. (2019) разглеждат операционните рискове в рамките на системата на полицията.

Второ, отчитаме засилен фокус върху информационните системи и създадените от тях кибер-рискове като ключов компонент от общия оперативен риск на организацията. Egan et al. (2019) подчертават, че кибер-рисковете вече се превръщат в един от най-важните източници на операционни рискове. Поради сравнителната си новост, за тях не съществуват стандартизирани модели за оценка и управление. Затова и Egan et al. (2019) предлагат ком-

бинация между две съществуващи рамки за идентификация и оценка на рисковете в информационната сигурност – таксономията на форума на Главните директори по риска и стандартите на Националния институт за стандарти и технологии в САЩ. Те разработват три основни сценария, демонстрирайки модела си: изтичане на чувствителни данни чрез служител на организацията, кибер изнудване и хакване на устройство за дистанционно предаване на данни. На този етап данните за кибер-рисковете са сравнително ограничени и някои от оценките по необходимост са субективни. Evans (2019) обосновава важността на кибер-рисковете с факта, че над 85% от активите на съвременните организации са цифрови. Допълнително, той (ibid.) предлага и пълноценна рамка за управление на този тип рискове.

Kashyap & Wetherilt (2019) подчертават, че кибер-рисковете се отличават спрямо останалите типове операционни рискове поради това, че проблемите, свързани с тях, се разпространяват с висока скорост и съществува значителна несигурност относно обхвата им. Допълнително, поради спецификата на кибер-рисковете, стимулите за изграждане на система за защита се разминават на индивидуално и на обществено ниво, което предполага и нуждата от известна регулация. Biener et al. (2018) обосновават кибер-рисковете като нов тип операционен риск, който подлежи на застраховане. Основните проблеми с този подход са сравнителната новост на кибер-рисковете, ограничените данни, нестабилните оценки на свързаните параметри и високата корелация с други типове рискове. Eling & Wirfs (2019) използват данни от база данни с операционни рискове, за да оценят 1579 специфични кибер-рискове и да ги остойностят адекватно, използвайки методи от теория на екстремните стойности. Допълнително, те (ibid.) подчертават два основни типа кибер-риск – ежедневни и катастрофални, и обосновават, че основният им източник е неизменно човешкият фактор. Някои автори подчертават и растящия риск от кибер-рискове по линия на нови технологии като интернет на нещата и предлагат системи за управлението им (вж. пр. Radanliev, 2019).

Трето, с увеличаването на обема от данни (Ward & Barker, 2013) се налага и използването на нови технологии за тяхното набиране, съхранение и обработка. В този смисъл, виждаме приложението на авангардни технологии за обработка на данни (пр. използване на нерелационни бази данни и неструктурирани данни), както и навлизане на нови методи, вдъхновени от машинното самообучение. Сред тях си струва да отбележим и засиления интерес към Бейсовата статистика и теорията на размитите множества. Pena et al. (2018) представят подход, който да интегрира както количествени, така и качествени данни от вътрешни и външни източници. Те (ibid.) използват основни резултати от теорията на размитите множества, за да изведат метрики за операционния риск. Pena et al. (2018b) показват как към този подход могат да се интегрират и Монте Карло методи за избор на извадката, използвана за оценка на параметрите.

Ljungblom & Bergren (2018) използват дълбока невронна мрежа, за да клъстерират различни наблюдения и по този начин да оценят операционния риск. Khan et al. (2018) използват обектно-ориентирана Бейсова мрежа в своя подход за управление на операционния риск в морското корабоплаване, като с нея интегрират широк набор от оперативни данни и изчисляват вероятността за настъпване на рисково събитие (сблъсък на кораб с ледена блок). Azar & Dolatabad (2019) също използват Бейсова мрежа, като демонстрират възможността за комбинация между входни данни от размито множество, които впоследствие захранват Бейсова мрежа за изчисляване на

метрики за операционния риск. Този модел се прилага и валидира в Иранска банка със задоволителни резултати. Xu et al. (2019) предлагат комбинация от интензивно набиране на данни, комбинирани със смесен гаусов модел като подход за управление на риска. Li et al. (2019) също предлагат хибриден модел за управление на операционния риск, като стъпват върху метода за анализ на функционалния резонанс. Макар този подход да има силно застъпен качествен елемент, той подчертава важността от междудисциплинарното разбиране и използване на различни допълващи се подходи за управление на операционния риск.

Като цяло се забелязва ясно изразена тенденция за навлизане и на авангардни методи от областта на машинното обучение за целите на оценката и управлението на операционните рискове. Paltrinieri et al. (2019) предлагат използването на такива методи за провеждането на детайлна рискова оценка. По-конкретно, те (ibid.) използват дълбока невронна мрежа, за да разгледат рисковата експозиция на проект, включващ платформа за добив на нефт. Резултатите от модела, базиран на невронна мрежа, са задоволителни и показват нейните добри възможности. Milkau & Bott (2018) обосновават, че алгоритмите за машинно обучение са се доказали в областта на реактивното управление на риска, но те имат широки възможности и за проактивно (прогностично) управление на операционните рискове. Тук подчертаваме, че проактивното управление реално е именно това, което има потенциал да генерира най-висока добавена стойност за съвременните организации.

В своя книга от 2019 г., Aziz & Dowling (2019) представят значително разширен набор от методи от машинното обучение и изкуствения интелект, които могат да бъдат използвани за управление на риска. По-специално, те се фокусират върху кредитния риск, пазарния риск, операционния риск и риска от несъответствие. Макар да има практически предизвикателства пред използването на авангардни количествени методи и изкуствен интелект за управление на рисковете, е силно вероятно това да бъде доминиращият изследователски и практически подход през следващите десетилетия. На този етап вече се виждат и определени изследвания с тази насоченост. Baryannis et al. (2019) обосновават използването на изкуствен интелект при управлението на риска и очертават основни сфери на приложение в областта на логистиката и управлението на веригата на доставките. Chandrinos et al. (2018) предлагат два инструмента за управление на риска, базирани на изкуствения интелект. Първият от тях използва машинно-генерирани дървета за вземане на решения, а вторият – изкуствени невронни мрежи. Тези подходи са директно трансферни към широк спектър от потенциални ситуации и задават общата посока на развитие на подходите за управление на операционните рискове предвид новите технологии и тенденции в областта.

Четвърто, забелязва се по-ясно осъзнаване на това, че различните рискови групи са интегрирани, преплитащи се и значително влияещи си една на друга. В този смисъл, немалко изследвания се фокусират върху търсене на общите характеристики на различните типове рискови експозиции и изследват начини за тяхното интегрирано управление. Rezapour et al. (2018) използват стохастичен математически модел, за да покажат корелациите между подходите за намаляване на стратегическия и на операционния риск, като показват значителна свързаност между двата типа категории. В сходен дух, Markou & Corsten (2018) показват свързаността между операционните и финансовите рискове и съветват ръководството на организацията да осмисли тяхната допълняемост, като за целта предприеме интегрирани действия по управле-

ние на риска. Bandaly et al. (2018) представят алтернативен модел за интегрирано управление на организационните рискове, който включва валутен риск, ценови риск и несигурност в търсенето. Използвайки финансови и операционни методи, те (ibid.) показват ползата от управление на риска чрез хеджиране в контекста на веригата на доставките. Farr & Bailey (2019) предлагат и обединяването на процесите по управление на операционния риск и тези по обезпечаване на продължителността на бизнес дейностите, като виждат значителна стойност в комбинираните управленски подходи.

Ko et al. (2019) изследват връзката между операционните рискове, кредитните рискове и качеството на корпоративното управление. Използвайки многомерни регресии, те показват, че по-високите нива на операционен риск са обвързани с по-висока вероятност за необслужване на поети кредити, както и с по-лоши финансови резултати на организацията. От друга страна, Ko et al. (2019) достигат и до извода, че по-доброто корпоративно управление води до по-малко инциденти, свързани с операционен риск, подобри организационни резултати и намален кредитен риск. Neifar & Jarboui (2018) откриват, че и по-доброто корпоративно управление води до по-пълно представяне на информация за операционния риск на външни инвеститори, за които това създава значителна стойност.

Извън ясната връзка между операционните рискове и различните други типове рискове, видима във високите корелации между тях, операционните рискове на дадена организация могат да имат ефект и върху цялостната среда, в която тя осъществява своята дейност. Berger et al. (2019) показват, че нивото на операционен риск на дадена банкова група влияе и върху нивото на риска за системата като цяло. Това е особено валидно за системно-важни субекти и в случаите на редки събития с потенциално големи ефекти (събития от „дебелата опашка“ на разпределението). Подобни открития са интересни, тъй като показват възможността за диспропорционално намаляване на системния риск чрез адресиране на експозицията на отделни компоненти. Eckert et al. (2018) също моделират външните ефекти от операционните рискове и откриват, че рисковете от външни ефекти зависят силно от характеристиките на специфичната организация. Barakat et al. (2019) показват и че съществуват ефекти от начина на медийно отразяване на данните за операционния риск. Тези потенциално негативни ефекти са най-големи при липсата на ясно регулирана и количествена информация, която да успокои заинтересованите страни.

Pieket Weeserit & Spruit (2018) допълнително подчертават ползите от интегрираното управление на риска в единна информационна система. Те (ibid.) предлагат данните и процесите за широк обхват от рискове да бъдат обхванати от единна информационна система за управление на бизнес резултатите. Това би позволило интегриране на източниците на първични данни (пр. оперативни бази данни), инфраструктурата за съхранението им (пр. складове за данни), процесите по обработка (извличане, обработка, зареждане), аналитичните процеси (доклади, табла с показатели, статистически измервания и модели) и използването на всички тези информационни ресурси за вземане на организационни решения в съответствие със стратегическите цели на организацията. От една страна, този подход стъпва на изведената висока корелация (0.78) между зрелостта на процесите по управление на операционните рискове и използването на информационни системи за управление на резултатите. От друга страна, той подчертава възможността за подобряване на дейностите, предполагащи решения в условия на несигурност, чрез информационни системи.

Основни препоръки и заключение

През последните две десетилетия наблюдаваме ясно изразена промяна на социално-икономическата среда и технологичните възможности на съвременните организации. От една страна, растящата комплексност увеличава рисковата експозиция към широк набор от различни типове операционни рискове (Chernobai et al., 2018), но от друга страна тя създава и нови възможности за тяхното по-ефективно управление. Това налага и преосмислянето на сега доминиращите подходи за целта, като новите подходи следва в максимална степен да включват възможността за анализ на големи масиви от данни и автономно вземане на решения и предприемане на действия от страна на автоматизирани информационни системи.

На първо място, това е неизбежно поради глобалните развития на пазара на труда и изискванията на съвременната среда. Наблюдаваме остро изразен недостиг на квалифицирана работна ръка на глобално ниво (Wojcik, 2018), паралелно с растящите изисквания към организациите за увеличение на продуктивността в среда на активна международна конкуренция. На практика, недостигът на достатъчно експертиза означава растяща необходимост от автоматизация на основни бизнес процеси. От друга страна е ясно изразена тенденцията и осъзната необходимостта от персонализация на всеки продукт и услуга, като това важи с особена сила за такива, предлагани в дигитална среда. Преминаването от напълно стандартизирани към високо персонализирани продукти и услуги предполага индивидуално и нарочно внимание към всяка инстанция на бизнес процесите, които ги създават. На практика, това е невъзможно за ценово-ефективно изпълнение от човешки експерти и предполага използването на автоматизирани информационни системи.

На второ място, новите възможности и инструменти на дигиталната трансформация създават и нови възможности за подобряване на ефективността и ефикасността на процеса по управление на операционния риск чрез неговата цифровизация. Сред основните технологични развития следва да подчертаем увеличената способност за набиране на големи масиви от данни чрез транзакционни системи, датчици, сензори и умни устройства, както и подходящи технологии за тяхното съхраняване и паралелна обработка (пр. нерелационни бази данни и архитектура за езеро за данни, вж. Schmarzo, 2015). Към това добавяме и развитието на усъвършенствани алгоритми за машинно обучение (надзиравано и ненадзиравано такова), които водят до модели с висока прогностична сила и могат да бъдат приложени в мащаба, изискван от експоненциално растящите големи масиви от данни. Прилагането на подобна авангардна аналитика вече носи значителни ползи на бизнеса (McAfee et al,, 2012; Wamba, 2017) и следва да бъде ефективно внедрена и в процеса по управление на операционните рискове.

На трето място, наблюдаваме и изместване на фокуса на изследванията в областта на операционните рискове, които да отчетат настъпилите промени в глобалната среда и в информационната архитектура на съвременните организации. Наблюдава се засилен фокус върху конкретни индустрии и рискови ситуации, като множество изследвания стъпват върху общи подходи и методологии за управление на риска и ги адаптират към конкретните нужди. Отчитаме това като израз на растящата тенденция към персонализация. Отчитаме и разширения фокус върху изследването на информационните системи на организацията и растящите кибер-рискове. И двете тенденции следва да бъдат интегрирани в управленските процеси във връзка с опе-

рационните рискове в съвременните организации.

Някои от съвременните изследвания апробират новаторски статистически алгоритми в полза на управлението на операционните рискове и търсенето на аномалии в големи масиви от данни (невронни и бейсови мрежи, дървета и гори за вземане на решения, алгоритми за клъстериране, машини с подкрепящи вектори). Отчитаме като особено важно преминаването от класически инструменти като визуален анализ и изчисляване на семпли коефициенти към подходящи методи, които могат успешно да бъдат приложени към значителни масиви от информация. Актуалните тенденции и технологичните възможности, от които може да се възползва съвременната организация, подчертават нуждите от оптимизация на ключови процеси по управление на риска.

В контекста на увеличената комплексност на стопанската среда се променят и типовете рискове, пред които са изправени организации и индивиди, както и интензитета им. Като пример, Chernobai et al. (2018) отбелязват, че с растящата сложност на финансовата среда се увеличават значително и операционните рискове пред банковите финансови институции. По подобен начин наблюдаваме и ръст на рисковите експозиции и на организациите от други сектори на икономиката, правителствата и дори отделните индивиди. Това предполага засилен интерес за управлението на тези рискове и използване в максимална степен на новите технологични развития в този процес. В този смисъл, общият поглед върху рисковия профил на организациите, фокусът върху специфични индустрии и казуси, както и по-пълното интегриране на ИКТ и авангардни методи от сферата на машинното обучение са ценни развития, които могат да спомогнат за генериране на значителна бизнес стойност.

Цитирани източници:

Анастасовски, Д., 2018. Съвременни аспекти при управлението на банковите рискове. *New Knowledge Journal of Science/Novo Znanie*, 7(1).

(Anastasovski, D., 2018. Savremenni aspekti pri upravlenieto na bankovite riskove. *New Knowledge Journal of Science/Novo Znanie*, 7(1))

Божинов, Б., 2016. Предизвикателства пред обезпечаване на информационната сигурност в търговските банки. *Бизнес управление*, 26(3), 7-23.
(Bozhinov, B., 2016. Predizvikatelstva pred obezpechavane na informatsionnata sigurnost v targovskite banki. *Biznes upravlenie*, 26(3), 7-23)

Видолова, М., & Георгиев, А., 2013. Рискът в банковата сфера – необходимост от идентифициране и управление. *Годишник на Стопанския факултет на Софийски университет „Св. Климент Охридски“*, 11, 51-64.

(Vidolova, M., & Georgiev, A., 2013. Riskat v bankovata sfera – neobhodimost ot identifitsirane i upravlenie. *Godishnik na Stopanskia fakultet na Sofiyski universitet “Sv. Kliment Ohdridski”*, 11, 51-64)

Вълканов, Н., 2018. Тенденцията към гранулиране или новата визия за нефинансовите рискове. *Известия на Съюза на учените – Варна. Серия Икономически науки*, 7(2), 34-43.
(Valkanov, N., 2018. Tendentsiata kam granulirane ili novata vizia za nefinansovite riskove. *Izvestia na Sayuza na uchenite – Varna. Seria Ikonomicheski nauki*, 7(2), 34-43)

Джарапов, П., 2018. *Рисковата култура на банките – значение, възможности за квантифициране, измерения в България.* София: Е-литера Софт.

(Dzharapov, P., 2018. *Riskovata kultura na bankite – znachenie, vazmozhnosti za kvantifitsirane, izmerenia v Bulgaria*. Sofia: E-litera Soft)

Димитрова, Р., 2008. Операционният риск в дейността на банките и някои аспекти от неговото управление. *Народностопански архив,* 2, 67-77.
(Dimitrova, R., 2008. Operatsionniat risk v deynostta na bankite i nyakoi aspekti ot negovoto upravlenie. *Narodnostopanski arhiv,* 2, 67-77)

Миланова, Е., 2012. Новата философия на Базел III. *Електронно списание Диалог,* (01), 1-46.
(Milanova, E., 2012. Novata filosofia na Bazel III. *Elektronno spisanie Dialog*, (01), 1-46)

Миланова, Е., 2019. Време ли е за Базел IV и какви са ефектите върху банките в България. *Икономически и социални алтернативи*, (1).
(Milanova, E., 2019. Vreme li e za Bazel IV i kakvi sa efektite varhu bankite v Bulgaria. *Ikonomicheski i sotsialni alternativi*, (1))

Милинов, В., 2010. Нерегулираното ипотечно кредитиране и кризата. *Бизнес управление*, 20(2), 104-114.
(Milinov, V., 2010. Nereguliranoto ipotechno kreditirane i krizata. *Biznes upravlenie*, 20(2), 104-114)

Минасян, Г., 2012. Анализ на банковата дейност. София: Институт за икономически изследвания на БАН.
(Minasyan, G., 2012. Analiz na bankovata deynost. Sofia: Institut za ikonomicheski izsledvania na BAN).

Стефанова, И., 2013. Банкова практика за сигурност на кредитите. *Икономическа мисъл*, (5), 90-108.
(Stefanova, I., 2013. Bankova praktika za sigurnost na kreditite. *Ikonomicheska misal*, (5), 90-108)

Ajina, M.A., Yousefi, B., & Zaidi, A.K., 2018. Structural Rules for Sound Business Process Implemented by UML Activity Diagram. In *Disciplinary Convergence in Systems Engineering Research* (pp. 911-930). Springer, Cham.

Akgün, M., 2018. The Operational Risk Assessments in Manufacturing Industry. In *Global Business Expansion: Concepts, Methodologies, Tools, and Applications* (pp. 653-675). IGI Global.

Azar, A., & Dolatabad, K.M., 2019. A method for modelling operational risk with fuzzy cognitive maps and Bayesian belief networks. *Expert Systems with Applications*, 115, 607-617.

Azevedo, A.I.R.L., & Santos, M.F., 2008. KDD, SEMMA and CRISP-DM: a parallel overview. *IADS-DM*.

Aziz, S., & Dowling, M., 2019. Machine Learning and AI for Risk Management. In *Disrupting Finance* (pp. 33-50). Palgrave Pivot, Cham.

Bandaly, D., Shanker, L., & Şatır, A., 2018. Integrated Financial and Operational Risk Management of Foreign Exchange Risk, Input Commodity Price Risk and Demand Uncertainty. *IFAC-PapersOnLine*, 51(11), 957-962.

Bank of International Settlements, BIS, 2001. *Working Paper on the Regulatory Treatment of Operational Risk.* Basel: BIS.

Barakat, A., Ashby, S., Fenn, P., & Bryce, C., 2019. Operational risk and reputation in financial institutions: Does media tone make a difference? *Journal of Banking & Finance*, 98, 1-24.

Baryannis, G., S. Validi, Dani, S., & Antoniou, G., 2019. Supply chain risk management and artificial intelligence: state of the art and future research directions. *International*

Journal of Production Research, 57(7), 2179-2202.

Basel Committee on Banking Supervision, BCBS, 2017. *High-level summary of Basel III reforms*. Switzerland: BIS.

Basel Committee on Banking Supervision, BCBS, 2006. *International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. Comprehensive Version, Basel Committee on Banking Supervision. http://www.bis.org/publ/bcbs128.htm

Berger, A. N., Curti, F., Mihov, A., & Sedunov, J., 2018. Operational Risk Is More Systemic than You Think: Evidence from US Bank Holding Companies. *Available at SSRN 3210808*.

Biener, C., Eling, M., & Wirfs, J. H., 2018. Insurability of cyber risk. *Methodology*, 9.

Cabena, P., P. Hadjinian, R. Stadler, J. Verhees, A. Zanasi, International Business Machines Corporation (San Jose, California)., & International Technical Support Organization (Sa Jose, California, 1997. Discovering data mining: from concept to implementation (p. 27). New Jersey: Prentice Hall PTR.

Chandrinos, S. K., Sakkas, G., & Lagaros, N. D., 2018. AIRMS: A risk management tool using machine learning. *Expert Systems with Applications*, 105, 34-48.

Chapman, P., J. Clinton, R. Kerber, T. Khabaza, T. Reinartz, Shearer, C., & Wirth, R., 2000. CRISP-DM 1.0 Step-by-step data mining guide. US: SPSS Inc.

Chernobai, A., Ozdagli, A. K., & Wang, J., 2018. Business complexity and risk management: evidence from operational risk events in US bank holding companies. *Available at SSRN 2736509*.

Chernobai, A., Rachev, S., & Fabozzi, F., 2007. Operational Risk. A Guide to Basel II Capital Requirements, Models and Analysis, John Willey & Sons. *Inc., March*.

Cipriano, N. A. A., 2018. The Effects of Internal and External Factors in Manufacturing Industry Towards Operational Risk. *Available at SSRN 3181623*.

Connolly, T. M., & Begg, C. E., 2005. Database systems: a practical approach to design implementation, and management. Pearson Education.

Crouhy, M., Galai, D., & Mark, R., 2001. *Risk Management*. New York: McGraw-Hill.

Crouhy, M., Galai, D., & Mark, R., 2006. *The essentials of risk management* (Vol. 1). New York: McGraw-Hill.

Dåderman, A., & Rosander, S., 2018. Evaluating Frameworks for Implementing Machine Learning in Signal Processing: A Comparative Study of CRISP-DM, SEMMA and KDD.

Deutsche Bank, 2005. Annual Report. Frankfurt: Deutsche Bank.

Eckert, C., Gatzert, N., & Heidinger, D., 2018. Empirically assessing and modeling spillover effects from operational risk events in the insurance industry. Working Paper, Friedrich-Alexander University Erlangen-Nürnberg (FAU).

Egan, R., Cartagena, S., Mohamed, R., Gosrani, V., Grewal, J., Acharyya, M., & Meghen, P., 2019. Cyber operational risk scenarios for insurance companies. *British Actuarial Journal*, 24.

Eling, M., & Wirfs, J., 2019. What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272(3), 1109-1119.

Embrechts, P., Furrer, H., & Kaufmann, R., 2003.Quantifying regulatory capital for operational risk. *Derivatives Use, Trading and Regulation*, 9(3), 217-233.

Embrechts, P., Mizgier, K., & Chen, X., 2018. Modeling operational risk depending on co-

variates: an empirical investigation. *Journal of Operational Risk*, 13(3).

Evans, A., 2019. Managing Cyber Risk. Routledge.

Farr, M., & Bailey, D., 2019. Uniting business continuity management and operational risk management. *Journal of business continuity & emergency planning*, 12(4), 294-300.

Hartini, R., Hartoyo, S., & Sasongko, H., 2018. The measurement of operational risk capital costs with an advanced measurement approach through the loss distribution approach (A case study in one of the Indonesia's state-owned banks). *Competition and Cooperation in Economics and Business.*

Heaton, R., Bryant, R., & Tong, S., 2019. Operational risk, omissions and liability in policing. *The Police Journal*, 92(2), 150-166.

Hoyle, D., 2017. ISO 9000 Quality Systems Handbook-updated for the ISO 9001: 2015 standard: Increasing the Quality of an Organization's Outputs. Routledge.

Jarrow, R.A., 2008. Operational risk. *Journal of Banking & Finance,* 32(5), 870-879.

Jorion, P., 2000. Value-at-Risk: The New Benchmark for Managing Financial Risk, 2nd ed. New York: McGraw-Hill.

Kashyap, A. K., & Wetherilt, A., 2019. May. Some Principles for Regulating Cyber Risk. In *AEA Papers and Proceedings* (Vol. 109, pp. 482-87).

Khan, B., Khan, F., Veitch, B., & Yang, M., 2018. An operational risk analysis tool to analyze marine transportation in Arctic waters. *Reliability Engineering & System Safety*, 169, 485- 502.

King, J. L., 2001. Operational Risk: Measurement and Modelling, John Wiley & Sons, New York.

Ko, C., Lee, P., & Anandarajan, A., 2019. The impact of operational risk incidents and moderating influence of corporate governance on credit risk and firm performance. *International Journal of Accounting & Information Management*, 27(1), 96-110.

Kopp, A. M., & Orlovskyi, D. L., 2018. AN APPROACH TO BPMN BASED BUSINESS

PROCESS MODELS ANALYSIS AND OPTIMIZATION. *Radio Electronics, Computer Science, Control*, (2).

Kroenke, D., Gemino, A.C., & Tingling, P.M., 2012. *Experiencing MIS*. Pearson.

Larose, D. T., & Larose, C. D., 2014. Discovering knowledge in data: an introduction to data mining. John Wiley & Sons.

Leone, P., & Porretta, P., 2018. Introduction to the Work and Operational Risk. In *Measuring and Managing Operational Risk* (pp. 1-23). Palgrave Macmillan, Cham.

Leone, P., Porretta, P., & Vellella, M. (Eds.), 2018. Measuring and Managing Operational Risk: An Integrated Approach. Springer.

Li, W., He, M., Sun, Y., & Cao, Q., 2019. A proactive operational risk identification and analysis framework based on the integration of ACAT and FRAM. *Reliability Engineering & System Safety*, 186, 101-109.

Ljungblom, L., & Berggren, J., 2018. Using Self-Organizing Maps to Identify Operational Risk. Thesis: Lund University & Svenska Handelsbanken AB. Stockholm.

Lu, J., 2018. Data Science in the Business Environment: Skills Analytics for Curriculum Development. In International Conference on Machine Learning, Optimization, and Data Science (pp. 116-128). Springer, Cham.

Markou, P., & Corsten, D., 2018. Financial and Operational Risk Management in the Gold Mining Industry. *Available at SSRN*

3185747.

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D., 2012. Big data: the management revolution. *Harvard business review*, 90(10), 60-68.

Milkau, U., & Bott, J., 2018. Active Management of Operational Risk in the Regimes of the "Unknown": What Can Machine Learning or Heuristics Deliver?. *Risks*, 6(2), 41.

Moosa, I.A., 2007. Operational risk: A survey. *Financial Markets, Institutions & Instruments*, 16(4), 167–200.

Neifar, S., & Jarboui, A., 2018. Corporate governance and operational risk voluntary disclosure: Evidence from islamic banks. Research in International Business and Finance 46: 43-54.

Paltrinieri, N., Comfort, L., & Reniers, G., 2019. Learning about risk: Machine learning for risk assessment. *Safety Science*, 118, 475-486.

Peña, A., Bonet, I., Lochmuller, C., Patiño, H.A., Chiclana, F., & Góngora, M., 2018a. A fuzzy credibility model to estimate the operational value at risk using internal and external data of risk events. *Knowledge-Based Systems*, 159, 98-109.

Peña, A., Bonet, I., Lochmuller, C., Chiclana, F., & Góngora, M., 2018b. Flexible inverse adaptive fuzzy inference model to identify the evolution of operational value at risk for improving operational risk management. *Applied Soft Computing*, 65, 614-631.

Power, M., 2005. The invention of operational risk. *Review of International Political Economy*, 12(4), 577-599.

Radanliev, P., De Roure, D. C., Nurse, J.R., Burnap, P., Anthi, E., Ani, U., & Montalvo, R.M., 2019. Cyber risk from IoT technologies in the supply chain–discussion on supply chains decision support system for the digital economy. Univ. Oxford.

Rezapour, S., Srinivasan, R., Tew, J., Allen, J. K., & Mistree, F., 2018. Correlation between strategic and operational risk mitigation strategies in supply networks. *International Journal of Production Economics*, 201, 225-248.

Schmarzo, B., 2015. Big Data MBA: Driving Business Strategies with Data Science. John Wiley & Sons.

Vose, D., 2008. Risk analysis: a quantitative guide. John Wiley & Sons.

Ward, J. S., & Barker, A., 2013. Undefined by data: a survey of big data definitions. arXiv preprint arXiv:1309.5821.

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J. F., Dubey, R., & Childe, S. J., 2017. Big data analytics and firm performance: Effects of dynamic capabilities. *Journal of Business Research*, 70, 356-365.

Wójcik, P., 2018. Shortage of Talents–a Challenge for Modern Organizations. *International Journal of Synergy and Research*, 6, 123.

Xu, G., Qiu, X., Fang, M., Kou, X., & Yu, Y., 2019. Data-driven operational risk analysis in E-Commerce Logistics. *Advanced Engineering Informatics*, 40, 29-35.

Yang, X., Haugen, S., & Paltrinieri, N., 2018. Clarifying the concept of operational risk assessment in the oil and gas industry. *Safety science,* 108, 259-268.

Yingqi, C., Chang, M., Khoo, S., Yap, J. & Muhamad, I., 2018. Operational Risk and Its Determinants: A Study on Logistics and Tranportation Industry in Malaysia. Available at *SSRN 3182283.*