UDC: 006.063:005.9 Info M str. 4-10

ИНТЕГРАЦИЈА МЕНАЏМЕНТА РИЗИКА КРОЗ ЗАХТЕВЕ СТАНДАРДА ИСО 9001:2015, ИСО/IEC 27001:2013 И ИСО 22301:2012
RISK MANAGEMENT INTEGRATION THROUGH ISO 9001:2015, ISO/IEC 27001:2013 AND ISO 22301:2012 STANDARD REQUIREMENTS

Ана Чобреновић, Др Младен Ђурић, Милица Рајковић

РЕЗИМЕ: Сврха овог рада је да сагледа на који се начин организације могу бавити ризицима у вези са квалитетом, безбедношћу информација и континуитетом пословања кроз координацију различитих метода за менаџмент ризика, као и да представи значај који менаџмент ризика има на данашње пословање. Рад ће анализирати захтеве стандарда ИСО 9001:2015, ИСО/IEC 27001:2013 и ИСО 22301:2014 који су у вези са менаџментом ризика. Рад ће на овај начин приказати интеграцију захтева претходно поменутих стандарда у једноставан систем који помаже компанији да сагледа и континуирано третира ризике. На основу сагледаних захтева стандарда, биће приказан скуп корисних алата и метода помоћу којих се може имплементирати интегрисани менаџмент ризика, уз његове користи и претње које се могу јавити у току имплементације.

КЉУЧНЕ РЕЧИ: менаџмент ризика, квалитет, сигурност информација, континуитет пословања,, интегрисани систем менаџмента

ABSTRACT: The main purpose of this paper is to indicate how the organization can deal with risks related to quality, information security and business continuity through the coordination of different risk management methods, and to present the importance of risk management for organizations nowadays. We analyzed the requirements of ISO 9001:2015, ISO/IEC 27001:2013 and ISO 22301:2014 related to risk management. This served to create a base for integrating the requirements of the above - mentioned standards into a simple system that helps organizations to examine and continually treat risks is shown through this paper. Furthermore, a set of useful tools and methods for implementation of integrated risk management, based on the perceived requirements of the standards, will be presented in this paper, along with benefits and threats that may occur during the implementation.

KEY WORDS: Risk management, quality, information security, business continuity, integrated management system

1. УВОД

Појам ризика, као стања у коме је могуће нежељено одступање од исхода којем се надамо, одувек постоји у нашем окружењу, а самим тим, за данашње пословање, такво стање је неизбежно. Менаџмент ризика се огледа у систематичном спречавању наступања штетних догађаја и предузимањем добро усмерених мера у вези са било којим пословним активностима, финансијским или нефинансијским. (ИСО, 2015 а)

Управљање ризиком је битна пословна активност за предузећа свих величина. Имплементација управљања ризицима која је усклађена са захтевима стандарда за системе менаџмента представља велику олакшицу. Предузећа која ефикасно управљају ризицима ће успети и произвести висок квалитет производа и услуга, у складу са својим пословним циљевима.

Тренутни трендови у области сигурности и система менаџмента квалитета су орјентисани на тражење решења која делују превентивно на губитке кроз ефикасне и ефективне алате. Економске кризе, миграција и глобализација доносе сталне промене свих фактора пословања, и тако форсирају менаџмент да анализира и управља ризицима које препозна. Анализа ризика, на научној основи, може бити дефинисана као систематичан процес са итерацијама који подразумева процену и интерпретацију правих информација о анализи система и пратећим идентификованим опасностима. Имплицитним резултатима анализе, квалитативне или квантитативне, изражава се ниво ризика. Резултати нам помажу да доносимо одлуку о томе да ли је ризик прихватљив или не. (Pačaiova, Sinay, Nagyova, 2016)

Чињеница је да је менаџмент ризика као и менаџмент квалитета „пут, а не дестинација“ који води до сталног побољшања процеса пословања, од настанка појма квалитета па све до данас, а и убудуће. (Loosemore, Raftery, 2006.) Природа система менаџмента се заснива на Деминговом *PDCA (Plan-Do-Check-Act)* циклусу који наводи систем да се континуирано развија, преипитује и побољшава. Свако преиспитивање указује на неке корективе или превентивне мере или предлаже места за побољшања третмана ризика.

Кораци које менаџмент ризика подразумева различити аутори дефинишу кроз различите приступе. На пример: постављање и дефинисање циљева, предвиђање, планирање са одлучивањем, прибављање ресурса, организовање, мотивисање и инструисање, реализација, координација, адаптација и учење (Вујошевић, 2008.); или на пример: идентификација, анализа и управљање ризика (Ђапић, Лукић, Килибарда, 2012.).

Код сваког приступа се у основи, за потребе овог рада, могу издвојити следећи процеси::

- идентификација ризика,
- анализа и рангирање ризика,
- управљање ризика и
- контрола и праћење ризика.

2. КОНЦЕПТ РИЗИКА У СТАНДАРДИМА ЗА СИСТЕМЕ МЕНАЏМЕНТА КВАЛИТЕТА, СИГУРНОСТИ ИНФОРМАЦИЈА И КОНТИНУИТЕТА ПОСЛОВАЊА

2.1. *Концепт ризика у систему менаџмента квалитета*

У условима велике понуде производа и услуга на светском тржишту, задовољство корисника представља најбитнији фактор који обликује производе и услуге. ИСО стандарди серије 9000 од свог настанка 1987. године до сада, знатно су се развили. Прикупљањем бројних примера из пословних пракси, стандарди се проширују, ревидирају и иду у корак са временом. Чувена Аристотелова мудра изјава: „Оно што морамо да научимо да радимо, учимо радећи» потпуно описује развој стандарда. (Soyle, 1994.)

Да би корисник увек осећао да је у „сигурним рукама“ док користи одређени производ или услугу, потребно је, поред квалитета самог излазног производа или услуге, обезбедити и континуирану стабилност и контролу унутрашње организације компаније. Један од темеља сигурног и непрекидног пословања јесте ефективан менаџмент ризика који чини да је квалитет стално обезбеђен.

Нова верзија међународног стандарда специфицира захтеве за организацију да разуме сопствени контекст и да утврђује ризике као основу за планирање. То представља примену новог концепта „размишљања заснованог на ризику” у планирању и примењивању процеса система менаџмента квалитетом и помаже у одређивању обима документованих информација. Једна од кључних намена система менаџмента квалитета јесте да делује као превентивни „алат”.(ИСО, 2015 б)

2.2. *Концепт ризика у систему менаџмента сигурности информација*

Чињеница је да се у тзв. сајбер простору дешава мноштво нежељених догађаја. Важан циљ сваке организације је безбедност пословања, које у великој мери зависи од заштите информационих средстава, остале имовине и ресурса. Самим тим, увођење система менаџмента сигурности информација представља спровођење потребних мера за постизање задовољавајућег нивоа информационе сигурности унутар организације. Нагласак је на процесу управљања ризиком који поспешује избор превентивних и корективних мера и контрола које, ако су коректно имплементиране, обезбеђују да систем еволуира ка систему управљања променама у безбедном окружењу. (Кокић, 2016)

Ризик је у стандарду ИСО/ИЕЦ 27000 дефинисан као ефекат несигурности у очекивано, и исказан је нивоом ризика који је дефинисан као однос последица ризика и вероватноће њиховог настанка. (ИСО, 2016) Када говоримо о ризицима у сигурности информација, могу се уочити три сфере на које овај систем менаџмента утиче. То су: сигурност самих информација, безбедност информационих технологија и корпоративна (физичка) сигурност и заштита. Сигурност информација се односи на све облике података којима нека организација располаже. It relies on the classic Confidentiality-Availability-Integrity (CIA) triad for expressing security objectives. The CIA triad was introduced in the Nineties as a multipurpose, standard way to express security requirements concerning information assets. (Abdulhadi, Damiani, 2017.)

Менаџмент ризика је према стандарду ИСО/ИЕЦ 27001:2013 представљен кроз јасне захтеве за поступање са ризицима и различита правила поступања конципирана у виду контрола представљених у Анексу А овог стандарда. Контролама се обезбеђује правилна заштита и класификација информација. Ово се постиже и кроз сигурност информационих технологија која обухвата управљање рањивостима, инцидентима, конфигурацијама, мрежама, расположивошћу, *back-up* активностима, променама, као и свиме што се тиче функционалне сигурности рачунара и преносних уређаја (ISO, 2013). Копоративна (физичка) сигурност и заштита представља сегмент који се бави физичким аспектима заштите, проверама запослених, заштитом од крађа, насиља, саботажа и сваког другог штетног понашања или ситуације.

2.3. *Концепт ризика у систему менаџмента континуитета пословања*

Континуитет пословања према стандарду ИСО 22301:2012 представља способност организације да настави да испоручује производе или услуге на прихватљив и предефинисан начин након претрпљеног инцидента. Менаџмент континуитета пословања се дефинише као процес којим се идентификују потенцијалне претње по организацију и утицаји на пословање које те претње могу проузроковати, кроз шта се обезбеђују оквири за изградњу отпорности и способности за ефикасну реакцију на последице претњи, уз очување интереса свих кључних заинтересованих страна. (ИСО, 2012)

Упркос великој обазривости које намећу и системи менаџмента квалитета и системи менаџмента сигурности информација, опасности и даље постоје. На колико год прихватљив ниво се организације трудиле да доведу вероватноћу или ефекат ризика ти ризици и даље постоје. Уколико је неки ризик идентификован, а поготово уколико ризик није доведен до прихватљивог нивоа, вероватноћа за настанком тј. реализацијом могућег нежељеног исхода и даље постоји. Када посао доживи прекид, организације се суочавају са огромним финансијским и репутационим губицима.

Што је прекид пословања дужи, то је штета већа и озбиљнија. Систем менаџмента континуитета пословања наглашава потребу за добро дефинисаном структуром одговора на инциденте. Ово осигурава да када дође до инцидената, постоје спремни планови који дефинишу одговорности и конкретне акције које одговорна лица морају предузетикако би се систем вратио у нормално стање функционисања. У зависности од тога на које заинтересоване стране инциденти имају утицај, дефинишу се и адекватне шеме комуникација у току кризних ситуација, на пример са јавношћу или државним органима. (Танген, 2012)

3. ЗАХТЕВИ СТАНДАРДА ЗА СИСТЕМЕ МЕНАЏМЕНТА КОЈИ СУ ВЕЗИ СА МЕНАЏМЕНТОМ РИЗИКА

Стандарде генерално можемо посматрати као сагледане „најбоље праксе“ менаџмента неке области, које су проистекле из искуства компанија различитих делатности, окружења и услова, али и детаљних анализа и захтева који се на тржишту намећу. Стандарди су конципирани тако да представљају скуп препоручених захтева које организације треба да испуне како би достигле одговарајући ниво уређености сфера свог пословања као што су: менаџмент квалитета, сигурности информација, безбедности и здравља на раду, животне средине и слично.

Најновије верзије стандарда за системе менаџмента су у складу са Анексом ес-ел (Annex SL). Према овом анексу, стандарди морају да садрже предмет и подручје примене, нормативне референце, термине и дефиниције, и захтеве који се односе на:

- контекст организиције;
- лидерство,
- планирање;
- подршка;
- реализација оперативних активности;
- вредновање перформанси и
- побољшавање.

Кроз већину ових група захтева стандарда, што се посебно примећује код ИСО 9001:2015, прожимају се они који се односе на ризике, што ће у овом поглављу рада бити приказано.

3.1. *Захтеви стандарда за системе менаџмента квалитета*

У стандарду ИСО 9001:2015, захтеви који се односе на ризике и прилике, прожимају се кроз све тачке стандарда у већој или мањој мери. У Табели 1 су приказана места у стандарду на којима се помињу ризици:

Тачка	*Наслов тачке*	*Објашњење*
0	Увод	• Описује концепт размишљања заснованог на ризику.
4	Контекст организације	• На ову тачку се директно позива званични захтев за мере које се тичу ризика и прилика.
5	Лидерство	• Захтева се промовисање концепта размишљања базираног на ризику у целој организацији од стране највишег руководства. • Захтева се утврђивање ризика који утичу на усаглашеност производа/ услуге од стране највишег руководства.
6	Планирање	• Захтева да организација разматра питања која се односе на контекст и заинтересоване стране И да у складу са тиме утврђује ризике И прилике којима треба да се бави, као и да примењује и вреднује ефективност мера које се односе ња ризике И прилике.
7	Подршка	• Организација је у обавези да утврди и обезбеди неопходне ресурсе узимајући у обзир припадајуће ризике и ограничења.
8	Реализација оперативних активности (Функционисање)	• Захтева се примена мера за спречавање људских грешака.
9	Вредновање перформанси	• Експлицитно захтева утврђивање мера које се односе на ризике и прилике.
10	Побољшавање	• Захтева да организација, уколико је неопходно, поново преиспитује и ажурира ризике и прилике које је идентификовала.

Табела 1 - *Захтеви ИСО 9001:2015 у вези са ризицима*

Захтеви 6.1, 4.1. и 4.2 представљају најважније захтеве када је реч о ризицима. У захтеву *6.1* – Мере које се односе на ризике и прилике специфицира се да организација мора да планира мере које се односе на ризике, међутим, нема захтева који се односе на формалне методе за менаџмент ризика или документовани процес менаџмента ризика. Организација је одговорна за примену свог размишљања заснованог на ризику и за мере које предузима да би се бавила ризиком, укључујући и то да ли чува или не чува документоване информације као доказе свог утврђивања ризика.

Тачка 4. - *Контекст организације* је још једна од „новости“ у новој верзији стандарда за системе менаџмента квалитета. Уочавамо да пре него што се закорачи у даље захтеве, при самом почетку читања захтева стандарда, долази се до потребе за идентификацијом организационог окружења, али и свих интерних питања. Такође, на почетку је потребно и идентификовати све заинтересоване стране које имају утицаја на организацију ради лакшег и бржег испуњења њихових захтева. За примењивање овог захтева, постоје вишеструке методе, чији избор зависи од врсте и величине организације.

За потребе испуњења захтева из тачке 4.1. организација мора да идентификује интерна и екстерна питања која могу бити од утицаја на ефективност система менаџмента квалитета. Ово значи да се та питања касније „преводе“ у ризике и прилике за потребе испуњења захтева тачке 6.1. овог стандарда.

3.2. *Захтеви стандарда за системе менаџмента сигурности информација*

Стандард ISO/IEC 27001:2013 је конципиран као скуп захтева, који су због примене Анекса СЛ веома слични онима за системе менаџмента квалитетом. Мноштво тачака имају идентичан назив као и тачке стандарда ИСО 9001:2015, али се односе на разматрање тих тема у смислу сигурности информација. Такође, поред захтева (тачака и подтачака), постоји и Прилог А са великим бројем контрола које се односе на сигурност информација. У Табели 2 је дат приказ тачака стандарда ISO/IEC 27001:2013 који су у вези са ризиком (ISO, 2013):

Тачка	Наслов тачке	Објашњење
4	**Контекст организације**	• Утврђивање интерних и екстерних питања релевантних за систем менаџмента сигурности информација реферише на стандард ИСО 31000:2009 за системе менаџмента ризика; • Захтева се да организација утврђује заинтересоване стране релевантне за систем менаџмента сигурности информација.
6	Планирање	• Захтева се да организација дефинише и примењује процес оцењивања ризика по сигурност информација; • Захтева се да организација дефинише и примењује процес поступања са ризиком по сигурност информација на основу резултата оцењивања ризика
8	Функционисање	• Захтева се да организација дефинише и примењује процес поступања са ризиком по сигурност информација на основу резултата оцењивања ризика

Табела 2 - *Захтеви ИСО/IEC 27001:2013 у вези са ризицима*

Тачка 4. - *Контекст организације* је веома сличан ономе из ИСО 9001:2015, док су тачке 6. – Планирање и 8. – Функционисање преостале тачке у којима се спомињу ризици, и то тако што захтевају постојање јасног процеса оцењивања и поступања са ризицима којих није експлицитно било у ИСО 9001:2015.

Оцењене и анализиране ризике, потребно је упоредити са наведеним контролама и њиховиим циљевима из Прилога А и повезати их са утицајем на одговарајућу информациону имовину коју организација поседује. Уколико се препознат ризик поклапа са неком од контрола или може да угрози реализацију неког од наведених циљева, мере којима ће се тај ризик ублажити морају да обухвате све оне које стандард наводи у оквиру те контроле. Другим речима, мера ће обухватати најмање оно што захтева одговарајућа контрола из Прилога А.

3.3. *Захтеви стандарда за системе менаџмента континуитета пословања*

Иако ИСО 22301 такође има структуру коју прописује *Annex SL* и велики број истих захтева као и претходна два анализирана стандарда, важно је уочити захтеве у вези са ризицима по којима ће се овај систем у интегрисаном систему менаџмента ризика истаћи. Највише специфичних захтева који употпуњују слику управљања ризицима у односу на ИСО 9001 и ИСО/ИЕЦ 27001 се налазе у оквиру тачке 8 – Функционисање. Ови захтеви, као и други генерички захтеви у којима се наводе аспекти континуитета пословања објашњени су у Табели 3 (ISO, 2012):

Тачка	Наслов тачке	Објашњење
4	**Контекст организације**	• Захтева се да организација утврђује заинтересоване стране релевантне за систем менаџмента континуитета пословања.
5	**Лидерство**	• Руководство мора да доказује своју посвећеност учествовањем у: - дефинисању критеријума за прихватање ризика; - тестирању планова за континуитет пословања;
8	**Функционисање**	• Ова тачка стандарда детаљно објашњава да је потребно: - спровести анализу утицаја на пословање; - спровести оцењивање и рангирање ризика; - дефинисати стратегију континуитета пословања на основу резултата анализе утицаја претњи на пословање, као и обезбедити све потребне ресурсе за реализацију ове стратегије, а затим спроводити мере које смањују вероватноћу прекида пословања, скраћују период прекида или ограничавају прекид пословања; - утврдити процедуре и планове за континуитет пословања којима се одговара на потенцијалне инциденте и прекиде пословања; - спроводити редовна тестирања планова континуитета пословања.

Табела 3 - *Захтеви ИСО 22301:2012 у вези са ризицима*

Посебно је занимљиво истаћи да је контрола А.17 Аспекти сигурности информација код менаџмента континуитетом пословања из Прилога А стандарда ISO/IEC 27001:2013 веома блиска са овим стандардом, јер захтева да сигурност информација буде уграђена у систем менаџмента континуитетом пословања (ISO, 2013). Ова контрола даље захтева да се спроводи планирање континуитета сигурности информација, имплементира континуитет сигурности информација кроз одговарајуће процесе и документоване информације, као и да се спроводи верификација, преиспитивање и процена континуитета сигурности информација (ISO, 2013)

4. ИНТЕГРАЦИЈА МЕНАЏМЕНТА РИЗИКА

На који начин започети имплементацију система менаџмента и на који начин обухватити више система менаџмента одједном? Одговор на ово питање је интегрисани систем менаџмента. У претходним поглављима овог рада анализирани су захтеви стандарда за системе менаџмента квалитета, сигурности информација и континуитета пословања. Иако су сви ови стандарди по структури исти, обратили смо пажњу на места на којима се истиче менаџмент ризика, тј. који су то захтеви стандарда у вези са ризиком специфични за ИСО 9001, ИСО/ИЕЦ 27001 и ИСО 22301.

Интеграција система менаџмента подразумева надградњу једног система менаџмента другим, управо оним аспектима који су јединствени за тај систем менаџмента. Предмет овог рада је интеграција менаџмента ризика у стандардизованим системима менаџмента, те ће тако у овом поглављу на основу анализираних захтева три стандарда за системе менаџмента, бити дат приказ начина на који се менаџмент ризика може примењивати у организацији било ког типа, тако да задовољава захтеве наведена три међународна стандарда.

У Табели 4 су приказани аспекти на које је потребно обратити посебну пажњу приликом имплементације менаџмента ризика, према захтевима стандарда ИСО 9001:2015 за системе менаџмента квалитета, ИСО/ИЕЦ 27001:2013 за системе менаџмента сигурности информација и ИСО 22301:2012 за системе менаџмента континуитета пословања:

ИСО 9001:2015	ИСО/ИЕЦ 27001:2013	ИСО 22301:2012
Контекст организације	Контекст организације	Контекст организације
Размишљање засновано на ризику	CIA тријада	Примена Business Impact анализе
Сагледавање ризика у вези са заинтересованим странама и стејкхолдерима	Евалуација вероватноће и последице ризика	Примена стратегије континуитета пословања
Сагледавање ризика у вези са процесима	Примена планова третмана ризика и контрола из Анекса А	Примена Планова континуитета пословања

Табела 4 - *Главни аспекти менаџмента ризика за интеграцију стандардизованих система менаџмента*

Видимо да основу интеграције представља утврђивање контекста организације, тачније, њеног интерног и екстерног окружења и заинтересованих страна у вези са квалитетом, сигурношћу информација и континуитетом пословања. Када посматрамо менаџмент ризика одвојено од имплементације целокупног система манеџмента, може се рећи да је утврђивање контекста организације полазна тачка корака идентификације ризика.

Може се уочити да када се испуне захтеви стандарда ИСО 9001:2015 који су у вези са ризиком, остаје само надоградити сагледавањем кроз безбедност информација и континуитет пословања уз евалуацију њихове вероватноће појављивања, последица и утицаја на пословање, дефинисање начина третмана ризика, као и одредити посебан третман ризика који угрожавају континуитет пословања и одредити начин на који се поступа уколико се ризици реализују. У наставку овог поглавља предложене су анализе које могу подржати овакав начин интеграције менаџмента ризика.

4.1. *Примена интегрисаног менаџмента ризика*

Идентификација ризика је почетна и уједно најтежа фаза менаџмента ризика. Као почетна метода за идентификацију може се користити *brainstorming* метода како би се идентификовали ризици у вези са квалитетом, ефективношћу и ефикасношћу спровођења процеса заједно са власницима и извршиоцима процеса. У кораку идентификације битно је генерисати што више идеја у вези са потенцијалним непредвиђеним ситуацијама, било да су се оне већ догодиле или постоји могућност да се догоде, кроз сагледавање резултата SWOT и PEST анализа, али и помоћу benchmarking-a. Понекад је теже идентификовати ризике у вези са сигурношћу информација и континуитетом пословања без лица које имају експертизу у тим пољима, стога се као помоћ идентификацији може користити матрица за процену ризика креирана и попуњена од стране стручног лица за безбедност информација. За идентификацију ризика у вези са континуитетом пословања потребне су консултације са руководиоцем физичко-техничке заштите, специјалисте за корпоративну безбедност или особља задуженог за евакуацију и противпожарну заштиту како би се дефинисали уопштени ризици континуитета пословања.

Корак анализе и рангирања ризика обично се састоји из додељивања квалитативног описа или квантификованих вредности идентификованим ризицима. Анализа ризика је основа *FMEA* методе. Ова метода представља структурирани приступ ризицима и тако помаже пројектантима система да разумеју исходе и приоритете чак и пре формалног завршетка ана-лизе ризика. (Jenab, 2015) FMEA анализа се често користи за откривање могућих узрока техничко-технолошке природе, али у последње време, препозната је као погодна и за анализу отказа различитих врста система који се тичу пружања услуга. Ако постоји било какав систем као што је и систем менаџмента квалитета, FMEA анализу је могуће применити. У кораку анализе ризика је најважније јасно утврдити обим и значење оцена ризика како би се добили што прецизнији резултати. У овом кораку могуће је придружити и Анализу утицаја на пословање (Business Impact Analysis) тако што ће разматрати њени резултати и одлучивати шта је потребно учинити као активност за сузбијање ових ризика.

Управљање ризика треба да одговори на следећа питања: Како позитивни ефекти могу бити ојачани? Како се могу смањити или спречити нежељени ефекти на жељени резултат? На менаџменту организације је да утврди како ће поступити са анализираним ризиком, тј. које ће ризике прихватити, а за које ће дефинисати и спроводити одређене мере за њихово сузбијање. За ризике у вези са сигурношћу информација, према захтевима стандарда потребно је израдити Планове третмана ризика,, а за ризике који узрокују застој пословања потребно је израдити и редовно тестирати Планове континуитета пословања.

Контрола и праћење ризика треба да одговоре на питање како организација вреднује ефективност мера предузетих у фази управљања ризиком и како организација може остварити стално побољшавање у третманима ризика. Управо овај корак се односи на идентификацију нових и ре-евалуацију старих ризика како би се проценио ефекат спроведене мере и по потреби дефинисале додатне или кориговале већ утврђене мере.

У Табели 5 је дат приказ могуће комбинације алата и метода уз помоћ којих се интегрисани менаџмент ризика може применити:

	Систем менаџмента квалитета	Систем менаџмента сигурности информација	Систем менаџмента континуитета пословања
Идентификација ризика	*SWOT, PEST(EL), Brainstorming, Benchmark*	*SWOT, PEST(EL), Brainstorming, Benchmark*, предефинисане матрице	*SWOT, PEST(EL), Brainstorming, Benchmark,* предефинисане матрице
Анализа и рангирање ризика	*FMEA* табела (анализа)	*FMEA* табела (анализа)	*FMEA* табела (анализа), *Анализа утицаја на пословање*
Управљање ризика	*FMEA* табела (мере)	*FMEA* табела (мере), Планови третмана ризика	Планови континуитета пословања
Контрола и праћење ризика	Праћење примене мера из *FMEA* табеле (мере); поновни почетак процеса идентификације ризика	Праћење примене мера из *FMEA* табеле (мере)и спровођења Планова за третман ризика и њихова корекција; поновни почетак процеса идентификације ризика	Праћење спровођења Планова за континуитет пословања; поновни почетак процеса идентификације ризика

Табела 5 - *Корисни алати и методе за имплементацију интегрисаног менаџмента ризика*

4.2. *Претње по примену менаџмента ризика*

Да би се искористиле користи интегрисаног менаџмента ризика, нормално је да ће најпре доћи до многих проблема приликом његове имплементације. Када говоримо о систему менаџмента сигурности информација, постоје многе отежавајуће околности по његову ефективну имплементацију. Често се дешава да постоји недостатак експертизе и компетенци неопходних за бављење сигурношћу информација, на свим хијерархијским нивоима организације, док се намећу константне промене у виду реструктурирања, спајања организација, различитих аквизиција и алијанси. Свака од ових измена има велики утицај на сигурност информација. (Asheden, 2008)

Да би организације уопште схватиле значај бављења ризицима, потребно је створити одговарајућу интерну културу коју је често врло тешко постићи. Она се развија у складу са понашањем запослених и њиховој свести о ризицима, на исти начин као што се организациона култура развија у складу са понашањем запослених у организацији. Она је заснована на интеракцији запослених са информационом имовином и безбедним понашањем које примењују у контексту организационе културе. За потребе овог рада, култура ризика је дефинисана као навике, претпоставке, начела, вредности и знање које запослени и интересне стране имају у интеракцији са организационим системом и процедурама у било ком тренутку. Из интеракције произилазе прихватљиво или неприхватљиво понашање (нпр. инциденти). Култура ризика и сигурности информација долази временом. (Da Veiga, Eloff, 2009)

Наравно, код многих организације се јавља проблем недостатка времена за систематичан менаџмент ризика, из чега произилазе погрешна тумачења менаџмента ризика на различитих хијерархијским и организационим нивоима.

4.3. *Користи од примене интегрисаног менаџмента ризика*

Имплементација система менаџмента квалитета наводи организације да планирају своје кораке опрезно уз сагледавање свих чинилаца који могу угрозити ефикасно одвијање пословних процеса и тако смањити квалитет крајњих производа и услуга. Имплементација система менаџмента сигурности информација побољшава квалитет информационог система и сигурности информација генерално и подиже свест о сигурности међу запосленима, купцима, добављачима итд. Такође, доприноси бољој повезаности информационих технологија са пословањем. (Pelnekar, 2011) Систем менаџмента континуитета пословања осигурава да су организације увек спремне на брз одговор и повратак у оперативно стање уколико се догоде инциденти који су прекинули пословање. Планирање и тестирање планова континуитета пословања су активности којима се запослени уче да реагују у ванредним ситуацијама, и стога много лакше подносе кризне ситуације.

Да би организације имале више користи од система менаџмента, требало би да разумеју да на њихову имплементацију утичу стратегија пословања, величина и структура организације, окружење и промене у окружењу као и ризици који вребају из унутрашњег и спољашњег окружења организације. (Kaziliunas, 2012) Самим тим, интегрисани менаџмент ризика који се односе на квалитет пословања, сигурност информација и континуитет пословања, постепено постаје део сваког сегмента пословања. Принцип размишљања заснованог на ризику постаје део свакодневних активности, различитих пројеката, организационих измена и управљања ресурсима било које врсте. Ово значи да запослени постају свесни ризика које сви наведени сегменти пословања носе, и то у погледу квалитета, сигурности информација и континуитета пословања. На тај начин, активности и ресурси су заштићени и сагледане су препреке које могу одвратити организацију од достизања постављених циљева.

5. ЗАКЉУЧАК

Можемо закључити да су ризици постали један од кључних аспеката квалитета пословања. Када је сагледан појам менаџмента ризика из различитих углова, приказани су кораци менаџмента ризика, који су веома блиски универзалним корацима менаџмента и чувеном Деминговом *PDCA (P-планирај, D-уради, C-* исконтролиши*, A-* коригуј*)* циклусу.

Кроз испуњење захтева стандарда за системе менаџмента квалитета, лако се ствара основа за надградњу система аспектима менаџмента сигурности информација. Анализом захтева стандарда за системе менаџмента безбедности информација може се закључити да се на њих лако могу надовезати захтеви за системе менаџмента континуитета пословања. Ово даје назнаке начина на који се менаџмент ризика какав захтевају ова три стандарда може интегрисати у један ефективан и ефикасан систем избором одговарајућих алата

и метода за његову примену. Примена FMEA методе се показује као веома ефикасна и веома ефективна када јој се придруже и други алати као што су SWOT, PEST, brainstorming, benchmarking, Планови третмана ризика за сигурност информација и Планови континуитета пословања.

Полазна тачка система менаџмента квалитета, сигурности информација и континуитета пословања (али и других система менаџмента) представља контекст организације којим се сагледава све на чему се пословање једне организације „темељи" као и оно што га окружује. Даљом интеграцијом система менаџмента квалитета, сигурности информација и континуитета пословања ствара се један савремени оквир за безбедно и заштићено пословање.

Организациона култура која се заснива на свести о значају сигурности и безбедности ће смањити ризике по квалитет, информације и смањити ризике од лошег понашања и штетне интеракције са информациону имовину и неадекватно поступање у ванредним ситуацијама. Потребно је запосленима на прави начин показати прве ефекте оваквог система. Када запослени једном разумеју да менаџмент ризика није оптерећење, већ просто помоћ да се њихов свакодневни посао подигне на виши ниво, тада се може говорити о ефективној имплементацији менаџмента ризика.

Цикличним понављањем и сталним унапређењем мера и начина менаџмента ризика доказали смо да је то „пут, а не дестинација". Менаџмент ризика се „уграђује" у сваки пословни процес, и учи запослене да размишљају унапред, што говори о његовој неопходности пословању. Интеграцијом захтева стандарда за системе менаџмента квалитета, сигурности информација и континуитета пословања, добија се свеобухватан систем, способан за предвиђање и одговор организације било које врсте на ризике који се могу јавити унутар ње или у њеном окружењу.

REFERENCES

[1] Abdulhadi, S., E. (2017). Damiani. On inter-Rater reliability of information security experts. Khalif Journal Of Information Security And Applications, број 37. 101–111.

[2] Ashenden, Debi. (2008). Information Security management: A human challenge?. Information security technical report, број 13. 195-201.

[3] Da Veiga, A., J.H.P. Eloff. (2010). A framework and assessment instrument for information security culture. Computers & Security, издање 29, број 2. 196.-207.

[4] Ђапић, Мирко, Љубомир Лукић и Веда Килибарда. 2012. „Стандардизација у области менаџмента ризика." Међународна научна конференција МЕНАЏМЕНТ 2012.

[5] ISO, 2012. ISO 22301:2012 Societal security – Business continuity management systems – Requirements. Geneva: ISO copyright office

[6] ISO, 2016, *ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Geneva: ISO copyright office

[7] ИСО. 2015. СРПС ИСО 9000:2015 Системи менаџмента квалитетом – Основе и речник. Београд: Институт за стандардизацију Србије (а)

[8] ИСО. 2015. СРПС ИСО 9001:2015 Системи менаџмента квалитетом – Захтеви. Београд: Институт за стандардизацију Србије (б)

[9] ИСО, 2013. СРПС ИСО/ИЕЦ 27001:2013 Системи менаџмента безбедношћу информација – Захтеви. Београд: Институт за стандардизацију Србије

[10] Jenab, Kouroush, Sam Khoury, и Samuel Rodriguez, 2015. „Effective FMEA Analysis or Not?!", Strategic Management Quarterly, број 2

[11] Kaziliunas, Adolfas. 2012. „Problems while implementing quality management systems for a sustainable development of organizations".Ekonomika in vadyba: aktualijos ir perspektyvos. Број 4.

[12] Кокић, Момчило, П. Тасевски. (2016). „Примена стандарда ИСО/ИЕЦ 27001 као фактора конкурентске предности организација". ИНФОТЕХ-ЈАХОРИНА. infoteh.etf.unssa.rs.ba.

[13] Loosemore, Martin и John Raftery. 2006. Risk management in projects. Њујорк: Taylor & Francis

[14] Pačaiova, H., J. Sinay, A. Nagyova, (2017). Development of GRAM – A risk measurement tool using risk based thinking principles. Measurements, 100. 288.-296.

[15] Pelnekar, Charu. 2011. „Planning for and Implementing ISO 27001". ISACA JOURNAL, Volime 4

[16] Soyle, Allan. 1994. Meeting ISO 900 in a TQM world. Велика Британија: AJSL Publishing

[17] Tangen, S., D. Austin, 2012, Business continuity - ISO 22301 when things go seriously wrong, ISOВујошевић, Мирко. 2008. „Управљање ризицима као сегмент интегрисаног система менаџмента". Total Quality Management & Excellence

Ана Чобреновић, (Аутор): Мастер инжењер организационих наука, одсек Менаџмент квалитета и стандардизација; запослена у компанији MPC Holding од 2016. године на позицији Супервизор за интегрисани систем менаџмента.
Контакт: ana.cobrenovic@gmail.com
Област рада: систем менаџмента квалитета, сигурности информација, безбедности и здравља на раду, континуитета пословања, инжењеринг процеса и управљање ризицима у областима менаџмента, дистрибуције робе и изградње објеката.

Др Младен Ђурић, (коаутор): Доцент на Факултету организационих наука, предаје предмете: основе квалитета, систем менаџмента квалитетом, систем управљања здрављем и сигурношћу, управљање квалитетом услуга, трошкови квалитета, енаџмент за квалитет, модели друштвене одговорности предузећа и управљање квалитетом у јавној администрацији на основним, мастер и докторским студијама Факултета. Од 2007. године ради и као пројектни менаџер, координатор и члан тима у 20 научних, образовних и консултантских пројеката.
Контакт: djuricm@fon.com

Милица Рајковић, (коаутор): Студент основних студија на Факултету организационих наука, од 2017. године члан тима за продукцију медија центра Quality media station на Факултету организационих наука.
Контакт: rajkovicmilica@outlook.com
Област рада: менаџмент квалитета, контрола квалитета, вођење пројеката, маркетинг, писање чланака, управљање социјалним мрежама