АГЕНЦИЈА ЗА БАНКАРСТВО РЕПУБЛИКЕ СРПСКЕ

УПУТСТВО
ЗА ОБАВЉАЊЕ РЕВИЗИЈЕ ИНФОРМАЦИОНОГ СИСТЕМА У БАНКАМА ОД СТРАНЕ СПОЉНОГ РЕВИЗОРА

Бања Лука, новембар 2019. године

Садржај

Увод

Упутство за обављање ревизије информационог система у банкама од стране спољног ревизора доноси се на основу члана 22. став 1. тачка ђ. Закона о Агенцији за банкарство Републике Српске („Службени гласник Републике Српске“ број 59/13 и 4/17), те члана 6. став 1. тачка б. и члана 22. став 4. тачка л. Статута Агенције за банкарство Републике Српске ("Службени гласник Републике Српске" број 63/17).

1. Предмет

1) Упутством за обављање ревизије информационог система у банкама од стране спољног ревизора (у даљем тексту: Упутство) дају се детаљне смјернице, као и очекивања Агенције за банкарство Републике Српске (у даљем тексту: Агенција) везана за обављање спољне ревизије информационих система у банкама, у складу са обавезама које проистичу из Закона о банкама Републике Српске (у даљем тексту: Закон), Одлуке о управљању информационим системима у банкама, Одлуке о управљању екстернализацијом, Одлуке о обављању спољне ревизије у банкама, Одлуке о условима и поступку издавања дозвола, одобрења и сагласности банкама које обављају дјелатност у Републици Српској, те у складу са добрим праксама.

2) У складу са законским и подзаконским актима наведеним у ставу 1. овог члана, привредно друштво за ревизију (у даљем тексту: спољни ревизор) дужно је сачинити извјештај о обављеној ревизији информационог система за потребе Агенције који, између осталог, треба да садржи информације о обављеној ревизији информационог система, оцјену стања и адекватности управљања тим системом, те би требао банци и Агенцији пружити квалитетне и потпуне информације о ризицима којима је тај информациони систем изложен.

3) Упутство се односи на банке и спољне ревизоре, који обављају ревизију информационих система у банкама, и имају за циљ побољшање квалитета ревизије информационих система, те боље разумијевање улога и одговорности банке и спољног ревизора у том процесу.

4) Агенција очекује да провођење ревизије, као и извјештај о обављеној ревизији буду у складу са наведеним у наставку овог документа, при чему се овај документ не може сматрати методологијом за обављање ревизије информационих система. Агенција ће, у поступку давања сагласности за обављање спољне ревизије информационог система, цијенити квалитет рада и поступања спољног ревизора, те усклађеност претходних ревизорских извјештаја са захтјевима из овог документа.

2. Именовање спољног ревизора

1) Начин избора спољног ревизора ради обављања ревизије информационог система, утврђен је Одлуком о управљању информационим системом у банци, Одлуком о обављању спољне ревизије у банкама и Одлуком о условима и поступку издавања дозвола, одобрења и сагласности банкама које обављају дјелатност у Републици Српској.

2) Услови и критеријуми које мора да испуњава спољни ревизор да би могао обављати ревизију информационогсистема банке дефинисани су Одлуком о условима и поступку издавања дозвола, одобрења и сагласности банкама које обављају дјелатност у Републици Српској и Одлуком о управљању информационим системима у банкама.

3) При провођењу спољне ревизије информационог система, очекује се да банка и спољни ревизор примјењују стандарде који су утврђени одредбама Закона о рачуноводству и ревизији Републике Српске, у мјери у којој су примјењиве (уговор, уговорни однос, уступање послова, потписивање извјештаја, временски период ангажовања, број запослених, радна документација, повјерљивост података, сукоб интереса и др.).

4) Скупштина банке, уз претходну сагласност Агенције, најкасније до 30. септембра текуће године, именује спољног ревизора који ће обавити ревизију информационог система за ту

годину. Уколико дође до измјене података на основу којих је спољни ревизор добио сагласност Агенције, дужан је одмах обавијестити Агенцију о измјени истих.

5) Спољни ревизор дужан је да Агенцији за сваку банку са којом је закључио уговор о обављању ревизије информационог система, доставити план обављања ревизије за ту пословну годину, најмање 30 дана прије почетка обављања ревизије, из којег су видљива подручја која су предмет ревизије, назначена имена лица која ће обављати ревизију и њихов ангажман, те вријеме трајања ревизије.

6) Извјештај о обављеној ревизији информационог система са стањем на дан 31. децембар претходне године је посебан извјештај, којег је банка дужна доставити Агенцији најкасније до 31. маја текуће године. Банка је обавезна Агенцији доставити оригиналан примјерак извјештаја на једном од језика који су у службеној употреби у Републици Српској и у електронској форми.

7) При обављању ревизије информационог система, спољни ревизор треба примјењивати међународне стандарде ревизије, Кодекс професионалне етике ревизора и правила ревизорске струке, те друга правила и прописе који регулишу ову област.

3. Компетенције особа које обављају ревизију

1) Лица која оперативно проводе ревизију информационог система морају посједовати одговарајућа знања, вјештине и искуства неопходна за обављање ревизорских задатака, која се стичу континуираном едукацијом (нпр. формалном едукацијом, те стручним усавршавањем и сертификовањем у областима везаним за ревизију информационих система и информационе системе), те одговарајуће радно искуство, како би се обезбиједило квалитетно и стручно обављање ревизије информационог система. Кључни чланови тима који ће обављати оперативни дио ревизије требају имати најмање по двије године радног искуства, у пословима обављања ревизије информационих система у банкама.

2) У свом раду, спољни ревизор треба примјењивати стандарде за ревизију информационих система, затим друге одговарајуће професионалне или индустријске стандарде, као и регулаторне захтјеве, који би обезбиједили могућност давања оцјене стања информационог система и адекватности управљања информационим системом.

3) Ако спољни ревизор нема запослене који имају одговарајућа знања и вјештине неопходне за обављање ревизије информационог система, спољни ревизор може ангажовати трећа лица, која посједују адекватне стручне квалификације (нпр. међународно признате сертификате за ревизију информационог система). Одговорност спољног ревизора према банци и Агенцији, не може се пренијети на лица која је спољни ревизор ангажовао.

4) Спољни ревизор и ангажована трећа лица требају бити независни, што подразумијева да у току ангажовања од стране банке не могу имати:
   1. било какав директан или индиректан финансијски интерес у банци или код било ког повезаног лица са банком и
   2. било какав други однос који може компромитовати његову независну оцјену односно консултантске услуге, ревизију сопственог рада (нпр. интерна ревизија), ревизија рада за који су били претходно одговорни и сл.

4. Одговорност спољног ревизора и банке

1) У процесу обављања ревизије информационог система, банка треба да упозна спољног ревизора са свим системима и апликацијама које користи у својим активностима. Банка је такође одговорна за достављање комплетне документације, која се односи на њен информациони систем, информација и документације коју спољни ревизор тражи, а која је се односи информациони систем банке, као и да овлашћено особље банке омогући спољном ревизору приступ ресурсима информационог система.

2) Спољни ревизор је одговоран да, на бази обављеног процеса ревизије и прикупљених ревизијских доказа, обезбиједи извјештај који садржи објективно и реално мишљење, те оцјену о стању информационог система и адекватности управљања информационим системом.

3) Уколико спољни ревизор за вријеме трајања ангажмана уочи недостатке, слабости или неправилности које представљају изразито високи ризик и које су истовремено критичне за безбједност информационог система банке, дужан је одмах обавијестити Агенцију.

5. Уговорни однос између банке и спољног ревизора

1) Уговор између банке и спољног ревизора треба јасно да дефинише све релевантне услове, права и обавезе, те одговорности уговорних страна, при чему минимално треба да садржи сљедеће одредбе:
   1. детаљан опис услуга које су предмет уговора,
   2. области које ће бити покривене ревизијом,
   3. уколико спољни ревизор ангажује подизвођача, потребно је навести податке о подизвођачу и/или физичким лицима који учествују у обављању оперативног дијела ревизије,
   4. методологије и процедуре које ће спољни ревизор користити,
   5. одговорност банке и спољног ревизора,
   6. ограничење одговорности и надокнада штете и
   7. обавезу заштите банкарске и пословне тајне.

6. Размјена информација између спољног ревизора и Агенције

1) Размјена информација и података између Агенције и спољног ревизора обавља се у писаној форми, путем одржавања састанака или по потреби на други начин договорен између Агенције и спољног ревизора.

2) Размјена информација и података по правилу се обавља током припреме и планирања ревизије, у току обављања ревизије и након потписивања извјештаја о обављеној ревизији, те у случајевима када су Агенцији потребне додатне информације и подаци за потребе надзора банке.

3) Ревизори су обавезни унаприједити своје извјештаје у складу са препорукама Агенције, те прегледати и одређене области информационог система, уколико их је Агенција проценила као критичне или од посебног значаја.

7. Ревизија информационог система

1) При провођењу ревизије информационог система, спољни ревизор даје оцјену стања и адекватности управљања информационим системом, при чему је дужан:
   1. служити се методама и поступцима за ревизију информационих система засновану на процјени ризика,
   2. дефинисати обим и план ревизије, на основу процјене ризика, прије почетка обављања ревизије информационог система,
   3. дефинисати дубину ревизије, у зависности од затеченог стања информационог система,
   4. провјерити и оцијенити стање информационог система и
   5. провјерити поштује ли банка важећу законску и подзаконску регулативу, а која се односи на информационе системе.

2) На основу ревизије информационог система спољни ревизор је дужан указати на значајне ризике којима је банка изложена.

8. Планирање ревизије информационог система

1) У циљу ефикасног обављања ревизије информационог система банке, неопходно је да спољни ревизор обави планирање ревизије, при чему треба узети у обзир најмање сљедеће:
   1. величину банке (тржишну и финансијску позицију и сл.),
   2. ризични профил банке, те склоност ка преузимању ризика,
   3. обим и сложеност пословних процеса,
   4. организацију банке (број запослених, организациону структуру, број организационих јединица и сл.),
   5. карактеристике информационог система (организациону и технолошку сложеност, хетерогеност софтверских и хардверских ресурса, обим и сложеност мрежне инфраструктуре и сл.),
   6. ниво екстернализовних активности које се односе на информациони систем банке (број пружалаца услуга и ниво значајности услуга које исти обављају, зависност од пружалаца услуга и сл.),
   7. извјештаје контролних функција са аспекта информационог система, одбора за управљање информационим системом, лица за безбједност информационог система и руководиоца организационе јединице за информациону технологију,
   8. извјештаје о претходно обављеним ревизијама информационог система од стране спољних ревизора,
   9. актуелне трендове везане уз технолошки напредак (нпр.: сајбер пријетње и слично) и
   10. усклађеност са регулаторним захтјевима.
2) Обим ревизије информационог система треба бити дефинисан на бази проведене процјене ризика. Притом је потребно рангирати подручја по критеријуму њихове ризичности, те у складу с тим посветити пажњу оним дијеловима и ресурсима информационог система који су неопходни за функционисање критичних/кључних пословних процеса банке.
3) Обим ревизије се може промијенити током обављања ревизије у складу са новим сазнањима о ризицима или другим чињеницама значајним за предмет ревизије.

9. Провођење ревизије информационог система

1) Током провођења ревизије информационог система спољни ревизор треба најмање да:
   1. утврди адекватност процеса управљања информационим системом,
   2. прегледа рад и активности контролних функција (посебно интерне ревизије информационог система, лица одговорног за безбједност информационог система, одбора за управљање информационим системом и сл.),
   3. процијени оперативну ефикасност процеса и успостављеног система унутрашњих контрола и
   4. провјери статус налаза раније обављених ревизија од стране спољних ревизора.
2) Спољни ревизор треба да провјери да ли су процеси који се односе на информационе системе (управљање инцидентима и корисничким захтјевима, управљање документацијом у вези с информационим системом, управљање развојем и промјенама, управљање контролама приступа, управљање заштитом од малициозног кода, управљање резервним копијама података, сајбер безбједност и сл.) адекватно успостављени, што укључује и провјеру нивоа документованости ових процеса интерним актима.
3) Потребно је нагласити да постојање интерних аката, као и њихова адекватност, не значи да су и процеси које исти регулишу адекватно успостављени. Због тога би спољни ревизор требао провјерити ниво имплементације наведених процеса у пракси, те њихову оперативну ефикасност, и дати објективну и реалну оцјену (мишљење) о истим.

10. Процјена стања информационог система

1) У циљу формирања објективне и реалне оцјене (мишљења) о стању информационог система и адекватности управљања истим, спољни ревизор треба извршити анализу архитектуре информационог система, технолошких карактеристика и конфигурација значајних ресурса информационог система.

2) Претходно наведено у ставу 1. овог члана подразумијева анализу дизајна мрежне инфраструктуре, технолошких карактеристика и конфигурација мрежних компоненти, архитектуру и конфигурације сервера, база података, анализу система за израду резервних копија и сл. У складу са наведеним, спољни ревизор би требао идентификовати оне ресурсе информационог система који су значајни за одвијање критичних/кључних процеса банке, као и оне ресурсе који су значајни са аспекта безбједности информационог система.

11. Употреба ревизорских алата

1) При обављању ревизије информационог система, спољни ревизор може користити одговарајуће ревизорске алате у циљу провјере ефикасности контрола уграђених у информациони систем, оцјене квалитета података и слично.

2) Употреба ревизорских алата, као и обим и начин њихове примјене, треба бити унапријед договорена са банком (прије закључења уговорног односа о обављању ревизије информационог система), с обзиром на могуће негативне посљедице примјене тих алата.

12. Извјештај о обављеној ревизији информационог система

1) Спољни ревизор треба по завршетку ревизије припремити извјештај који треба бити свеобухватан, објективан, заснован на чињеницама, прецизан и јасан.

2) У извјештају треба назначити назив банке и примаоце, обим, циљеве, период покривености ревизије, те природу и период провођења ревизије. Извјештај треба укључити налазе, ризике и препоруке, те уколико постоји суздржаност спољног ревизора, потребно је навести квалификације или ограничења у обиму које је спољни ревизор уочио током провођења ревизије.

3) Спољни ревизор треба у извјештају о обављеној ревизији информационог система обавезно навести имена лица, које су оперативно провеле ревизију информационог система банке, те њихов укупни ангажман на тим пословима.

4) Извјештај би требао да садржи минимално сљедеће:
   1. сажетак извјештаја
   2. дефинисање обима извјештаја и методологија
      - методологија/е за провођење ревизије (за процјену ризика и ревизију информационог система)
      - иницијална процјена ризика за одређивање обима ревизије
      - области информационог система које су биле предмет тестирања контрола
      - осврт на претходни извјештај о ревизији информационог система (статус препорука)
   3. резултате процјене ризика
      - преглед информационог система банке (архитектура система)
      - примијењени поступци процјене ризика
      - кључне компоненте информационог система укључене у обим ревизије
   4. налазе о контролама у информационом систему
      - област информационог система
      - запажања и ризици
      - оцјена ризика

- препоруке
- препоручени рокови за имплементацију препорука

5. усклађеност пословања банке са појединачним члановима Одлуке о управљању информационим системима у банкама и Одлуке о управљању екстернализацијом и
6. оцјене нивоа зрелости по областима информационог система.

5) У сажетку извјештаја о проведеној ревизији информационог система, требало би издвојити најзначајније налазе са припадајућим нивоима ризика и укупну оцјену стања и адекватности управљања информационим системом.

13. Налази, ризици и препоруке

1) У извјештају о обављеној ревизији информационог система треба јасно навести налазе, ризике и препоруке за свако подручје или дио информационог система који је био предмет ревизије.

2) Налаз ревизора је писмено објашњење неправилности, слабости, недостатака, грешака или потреба за побољшањима и промјенама које су откривене током ревизије. Налаз представља конструктиван критички коментар о одређеној радњи или непредузетој активности, што према мишљењу спољног ревизора представља препреку у остваривању жељених циљева на ефикасан и ефективан начин.

3) Налази које спољни ревизор наводи у извјештају требају испуњавати сљедеће:
   1. јасно и прецизно су идентификовани проблеми и недостаци утврђени током ревизије информационог система,
   2. садрже информације на који дио информационог система се односе (софтвер, хардвер, пословни процес и сл.),
   3. садрже назив стандарда или добре праксе, специфичне политике, процедуре или регулативе на коју се налаз односи,
   4. заснивају се на чињеничном стању утврђеном током ревизије информационог система,
   5. образложени су на објективан начин и у потпуности подржани ревизорским доказима и
   6. прецизни, довољно разумљиви и убједљиви.

4) Спољни ревизор би требао, гдје год је то могуће, разматрати кумулативни утицај слабости или одсуства контрола које се односе на исте пословне процесе или ресурсе, а који утичу на повећање укупног нивоа ризика информационог система. Такве налазе би требало међусобно повезати и груписати, те навести укупан ризик који из њих произилази.

5) Ако спољни ревизор утврди да за одређену област ревизије не постоје недостаци или да су утврђени недостаци од таквог значаја да их не треба навести у извјештају, информацију о томе да нису утврђени значајни недостаци је потребно навести у извјештају. Такви налази требају бити адекватно подржани ревизорским доказима, баш као и у случају констатовања слабости. У ситуацијама када спољни ревизор није прикупио довољно доказа како би испитао и оцијенио одређену област информационог система, спољни ревизор треба констатовати ту чињеницу.

6) Уколико постоје релевантни извјештаји за одређене области информационог система (нпр. пенетрациони тестови, извјештај о ревизији пружаоца услуга и сл.), спољни ревизор их може узети у обзир приликом оцјене ових области.

7) Спољни ревизор треба идентификовати и навести ризике који произилазе из утврђених налаза, те их образложити на начин да банка може на адекватан начин проценити могући утицај утврђених недостатака на пословање банке.

8) Спољни ревизор треба навести узроке постојеће ситуације, како би се уочени недостаци довољно појаснили. Опис и ниво ризика којима је изложен информациони систем треба јасно да упућује на могуће негативне посљедице на информациони систем, те на пословање банке.

9) Посљедице најчешће одражавају потенцијални финансијски губитак, неусаглашеност, нарушавање континуитета пословања, угрожену безбједност и сл. Спољни ревизор би требао објаснити значења нивоа ризика које користи у извјештају.

10) У препорукама би требало бити наведено стручно мишљење спољног ревизора о активностима које би банка требала провести како би ублажила ризике који произилазе из утврђених недостатака (налаза). Основне смјернице за писање препорука су сљедеће:
    1. препорука је стручна и конструктивна, те усмјерена на ублажавање ризика,
    2. представља логичан слијед онога што је представљено у налазу, те не уводи нове информације које нису представљене у оквиру наведеног чињеничног стања,
    3. не садржи опис активности које су већ предузете,
    4. не указује на специфична организациона и/или технолошка рјешења и
    5. предложен је адекватан рок за имплементацију препоруке.

11) Уколико су предложене активности за имплементацију препорука већ размотрене са управом банке, спољни ревизор треба укључити одговор управе и образложења у извјештај о обављеној ревизији информационог система.

12) Спољни ревизор је дужан да након обављене ревизије информационог система, сачини извјештај о обављеној ревизији за потребе Агенције, који укључује и свеукупну оцјену о стању информационог система и адекватности управљања информационим системом, те укаже на значајне ризике којима је банка изложена. Свеукупна оцјена се даје у сажетку извјештаја.

13) Оцјена из става 1. овог члана је описна и може имати једну од сљедећих вриједности:
    1. потпуно задовољавајуће,
    2. задовољавајуће,
    3. незадовољавајуће и
    4. у потпуности незадовољавајуће.

14) Приликом давања оцјене, спољни ревизор је дужан узети у обзир и усклађеност пословања банке са Законом о банкама, подзаконским актима који се односе на информациони систем (Одлука о управљању информационим системима у банкама и Одлука о управљању екстернализацијом), као и другом релевантном законском регулативом (нпр. Закон о зашити личних података и сл.). Приликом образлагања оцјене, спољни ревизор је дужан навести чињенице које су највише утицале на доношење оцјене стања информационог система и адекватности управљања информационим системом.

15) За сваку област информационог система која је била предмет ревизије, спољни ревизор треба дати појединачну описну оцјену у складу са методологијом коју користи (нпр. оцјена нивоа зрелости према *COBIT* методологији).

16) Агенција може од спољнег ревизора тражити додатне информације у вези са обављеном ревизијом.

14. Разлози за неприхватање података и информација из извјештаја о ревизији

1) Агенција може одбити извјештај о обављеној ревизији информационог система ако утврди да спољни ревизор у извјештају о ревизији информационог система није доставио податке и информације и дао оцјену за потребе Агенције у складу са Законом о банкама, Законом о рачуноводству и ревизији, прописима донесеним на основу ових закона и правилима струке или ако обављањем надзора над банком или на други начин утврди да подаци нису засновани на истинитим и објективним чињеницама. У овом случају Агенција може да захтијева:
    1. од спољног ревизора да податке допуни или измијени или
    2. од банке да именује другог спољног ревизора или да Агенција о трошку банке директно именује спољног ревизора који ће обавити ревизију информационог система.

15. Улога банке

1) Надлежни органи банке требају размотрити извјештај о обављеној ревизији информационог система, те се изјаснити о утврђеним налазима. При том могу коментарисати препоруке и ризике које је идентификовао спољни ревизор.

2) Банка би требала, на основу налаза наведених у извјештају о обављеној ревизији информационог система, проценити на који начин се наведени ризици уклапају у њен ризични профил и утврдити начин ублажавања наведених ризика.

3) Уколико банка процијени да може ублажити наведене ризике провођењем даљих активности, потребно је одредити које су то активности (мјере) које се требају провести, те дефинисати рокове и лица одговорна за провођење тих активности.

16. Прелазне и завршне одредбе

Ово упутство ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Српске".

Број: Д-14/19

Дана, 15.11.2019. год.

Директор

Раде Растока