Интегрални акциони план

за отклањање утврђених недостатака у ревизорском извјештају Grant Thornton д.о.о. Бања Лука за 2022. годину и прихватање препорука датих у Писму руководству Мјешовитог Холдинга „Електропривреда Републике Српске“

Требиње, Септембар 2023. године

Увод

Независни ревизор Grant Thornton извршио је преглед пословних књига свих Зависних предузећа и Матичног предузећа, као и консолидованог Мјешовитог Холдина „ЕРС", консолидованог ХЕТ, Консолидованог РиТЕ Угљевик, консолидованог ХЕ на Дрини, консолидованог ЕД Бијељина и ЕД Пале за 2022. годину и доставио појединачне извјештаје за Зависна предузећа, Матичног предузеће, консолидовани Извјештај за Мјешовити Холдинг и Писмо руководству.
Независни ревизор је појединачно за зависна предузећа и Матично предузеће дао слиједеће мишљење:

1. *МХ"ЕРС"Матично предузеће а.д. Требиње – позитивно мишљење - истицање питања - значајна неизвјесност у вези с временски неограниченим пословањем;*
2. *ЗП „Хидроелектране на Врбасу"а.д. Мркоњић Град –позитивно мишљење;*
3. *ЗП"Хидроелектране на Дрини „а.д. Вишеград – позитивно мишљење – истицање питања;*
4. *ЗП"Хидроелектране на Требишњици" а.д. Требиње –мишљење са резервом - значајна неизвјесност у вези с временски неограниченим пословањем;*
5. *„ХЕ Дабар" д.о.о. Требиње – мишљење са резервом - значајна неизвјесност у вези с временски неограниченим пословањем;*
6. *ЗП"Рудника и Термоелектране Гацко"а.д.Гацко – мишљење са резервом – истицање питања;*
7. *ЗП „Рудник и Термоелектрана Угљевик"а.д. Угљевик – негативно мишљење;*
8. *ЗП Електрокрајина а.д. Бања Лука - позитивно мишљење - истицање питања - значајна неизвјесност у вези с временски неограниченим пословањем;*
9. *ЗП Електродобој а.д. Добој – позитивно мишљење - истицање питања;*
10. *ЗП Електро-Бијељина а.д. Бијељина - мишљење са резервом - значајна неизвјесност у вези с временски неограниченим пословањем;*
11. *ЗП Електродистрибуција а.д. Пале - позитивно мишљење - - истицање питања - значајна неизвјесност у вези с временски неограниченим пословањем;*
12. *ЗП Електро- Херцеговина а.д. Требиње – мишљење са резервом – истицање питања - значајна неизвјесност у вези с временски неограниченим пословањем;*
13. *Зависно Друштво"ИРЦЕ"а.д. Источно Сарајево – позитивно мишљење;*
14. *„ХЕ Бистрица" д.о.о. – позитивно мишљење - значајна неизвјесност у вези с временски неограниченим пословањем;*
15. *ОИЕ БиМ Пале – позитивно мишљење – истицање питања;*
16. *ОИЕ Зворник – Позитивно мишљење;*
17. *„Руднг" д.о.о. Угљевик – позитивно мишљење;*

18. ОИЕ Љубиње - позитивно мишљење;

19. „ФЕ Требиње 2" д.о.о. Требиње — позитивно мишљење;

20. ВЕП Берковићи - позитивно мишљење.

21. Консолидовани финансијски извјештај МХ „ЕРС" Требиње - мишљење са резервом - значајна неизвјесност у вези с временски неограниченим пословањем.

У Писму руководству у дијелу финансијског извјештавања обрађена су слиједећа питања:

- *Судски спорови,*
- Очекивани кредитни губици - Потраживања од повезаних правних лица, потраживања од купаца, друга краткорочна потраживања - МСФИ 9 Финансијски инструменти
- Уговори о репрограму за задржана средства, Уговори о репрограму по основу накнада за ОИЕЕ и Уговори о зајму са повезаним правним лицима
- Начело сталности пословања
- Готовина и готовински еквиваленти
- *Залихе*
- Књижење ефеката исправке грешака из ранијег периода
- Полуњавање финансијских извјештаја - (наведени налази се односе Зависно друштво Електро Бијељину а.д. Бијељина).

У Писму руководству у дијелу информационих технологија обрађена су слиједећа питања:

- *Свеобухватна анализа информационог система;*
- *Контрола приступа добављача (налаз из 2020.)*
- *Консолидација инфраструктурних стандарда информационог система (налаз из 2021.),*
- *План континуитета пословања – BCP (налаз из 2021.),*
- *Примјена тикетинг система (налаз из 2021.),*
- *Замјена застарјелих СКАДА система (налаз из 2021.)*
- *Обезбјеђење ресурса за едукацију (налаз из 2021.),*
- *Сегментација мреже и изолација СКАДА система (налаз из 2021.),*
- *Коришћење старих оперативних система на рачунарима и серверима (налаз из 2021.),*
- *Софтверска подршка изради резервних копија (налаз из 2020.),*
- *Имплементација доменских политика (налаз из 2021.).*

Мјешовити Холдинг
Електропривреда Републике Српске Требиње

У Писму руководству је стављен акценат на одговорност менаџмента за циљеве и ограничења система интерних контрола.

Управа Мјешовитог Холдинга „ЕРС" Матично предузеће а.д. Требиње је предложила Интегрални акциони план у коме су прихваћене све препоруке дате од стране Независног ревизора. У Интегралном акционом плану предложене су мјере, носиоци активности и рокови за извршење.
Усвајањем овог Интегралног акционог плана, исти ће бити обавезујући за сва Зависна предузећа.

В. д. Генерални директор
Лука Петровић, дипл.инж.маш.

Датум: 15.09.2023. године
Број: 03/1-2992-7/23

1. Судски спорови

НАЛАЗИ РЕВИЗИЈЕ	ПРЕПОРУКА
Матично друштво и Зависна друштва - чланице Мјешовитог Холдинга су тужена страна у судским споровима са процијењеном вриједности на дан 31. децембра 2022. године у износу од 103.926 хиљада КМ. Даље, Холдинг је тужена страна у арбитражном спору у износу од 146 милиона еура који се води по Закону о арбитражи Републике Србије, покренутим од стране "Elektrogospodarstvo Slovenije – razvoj in inženiring" д.о.о. Марибор (наведени износ арбитражног спора се састоји од главног дуга и законске затезне камате) против Зависног друштва Рите Угљевик а.д. Угљевик. Холдинг на дан 31. децембра 2022. године није извршио резервисања по основу наведеног арбитражног спора, иако је према информацијама добијеним у току ревизије, арбитражни спор на дан 31. децембра 2022. године је у завршној фази и очекује се доношење Одлуке Арбитражног вијећа у корист тужиоца. У вези са горе наведеним, Арбитражно вијеће у Београду, донијело је Одлуку 03. јула 2023. године, којом се налаже Зависном друштву Рите Угљевик а.д. Угљевик да у року од 30 дана плати тужиоцу "Elektrogospodarstvo Slovenije – razvoj in inženiring" д.о.о. Марибор износ од 67 милиона EUR и затезну камату за овај износ почев од 01. јануара 2022. године па до исплате, а доношење Одлуке о висини акумулиране камате и трошкова арбитраже се оставља за будући период.	Препорука Ревизора је да руководство Холдинга и руководство Зависних друштава континуирано врши процјену ризика исхода судских и арбитражних спорова и врше адекватна резервисања по основу процјене ризика и исхода судских и арбитражних спорова. Такође, неопходно је да сви судски спорови буду објелодањени у Напоменама уз појединачне и консолидоване финансијске извјештаје, као и адекватне процјене исхода судских спорова.

ОДГОВОР РУКОВОДСТВА

Препорука се прихвата.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА

Управа Холдинга и управе Зависних предузећа континуирано требају вршити процјену ризика исхода судских спорова и вршити адекватна резервисања по основу процјене ризика.

Носилац активности: ***Управа МХ"ЕРС" и управе Зависних предузећа***

Рок: ***Континуирано***

2. Очекивани кредитни губици – Потраживања од повезаних правних лица, потраживања о купаца, друга краткорочна потраживања - МСФИ 9 Финансијски инструменти

НАЛАЗИ РЕВИЗИЈЕ	ПРЕПОРУКА
Током ревизије појединачних извјештаја (Матично друштво а.д. Требиње, Хе на Дрини а.д. Вишеград, Електро Добој а.д. Добој, Електро Херцеговина а.д. Требиње, и др.) констатовано је да се највећи дио потраживања односи на потраживања за електричну енергију и друго, од повезаних правних лица и која највећим дијелом датирају из ранијег периода. Матично друштво и Зависна друштва код признавања очекиваних кредитних губитака код потраживања од повезаних правних лица, користе дјелимично усвојене рачуноводствене политике, односно примјењује само став којим је дефинисано да се очекивани кредитни губици за повезана правна лица обрачунавају у проценту од 1% на ненаплаћена потраживања, односно приликом обрачуна очекиваних кредитних губитака не користи став 4. из члана 107. усвојених рачуноводствених политика који дефинише да се Потраживања од купаца, без обзира којој групи потраживања припадају, а чија потраживања са стањем на дан процјене износе 1.000.000 КМ и више, процјењују појединачно. Даље, током ревизије констатовано је да су Друга краткорочна потраживања на дан 31. децембра 2022. године исказана у износу од 12.705 хиљада КМ. Увидом у евиденције констатовано је да се највећим дијелом краткорочна потраживања односе на потраживања за затезну камату и потраживања од запослених. Зависно друштво Електро Бијељина није извршило обезвређење потраживања за затезну камату у износу од 133 хиљаде КМ, као ни потраживања од запослених у износу од 341 хиљаде КМ, што није у складу са усвојеним рачуноводственим политикама, као ни захтјевима МСФИ 9 Финансијски инструменти.	Препорука Ревизора је да Матично друштво и Зависна друштва у потпуности примјењује усвојене рачуноводствене политике и да на објективан и фер начин изврши обрачун очекиваних кредитних губитака за повезана правна лица. Даље, неопходно је да се преиспита и политика за обрачун очекиваних кредитних губитака за потраживања од купаца за електричну енергију.

ОДГОВОР РУКОВОДСТВА
Препорука се прихвата.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА
Формирати комисију на нивоу МХ ЕРС која ће преиспитати рачуноводствене политике за обрачун очекиваних кредитних губитака за потраживања од купаца за електричну енергију. ***Носилац активности:*** ***Управа Холдинга и Управе свих ЗП*** ***Рок:*** ***31.12.2023.***

3. Уговори о репрограму за задржана средства, Уговори о репрограму по основу накнада за ОИЕЕ и Уговори о зајму са повезаним правним лицима

НАЛАЗИ РЕВИЗИЈЕ	ПРЕПОРУКА
Током ревизије констатовано је да Матично друштво има више потписаних уговора о репрограму обавеза повезаним правним лицима и уговора о зајму повезаним правним лицима (Матично друштво а.д. Требиње, Хе на Дрини а.д. Вишеград, ХЕ на Требишњици а.д. Требиње, Електрокрајина а.д. Бања Лука, Електро Добој а.д. Добој, Електро Херцеговина а.д. Требиње, Рите Гацко а.д. Гацко и др.). Приликом евидентирања наведених уговора и обрачуна дисконта, Друштво је евидентирање укупног дисконта по основу Уговора о репрограму и Уговора о зајму евидентирало кроз текући период, односно финансијске приходе/расходе, што није у складу са захтјевима Концептуалног оквира финансијског извјештавања.	Препорука Ревизора је да Друштво изврши корекције евидентираног дисконта по основу уговора о репрограму обавеза од повезаних правних лица и Уговора о зајму са повезаним правним лицима, у складу са захтјевима МРС 8 Рачуноводствене политике, промјене рачуноводствених процјена и грешке и исти евидентира у складу са захтјевима Концептуалног оквира финансијског извјештавања.

ОДГОВОР РУКОВОДСТВА
Препорука се прихвата.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА
Ангажовати стручног консултанта који ће утврдити износе корекција и дати јасне инструкције у вези са књижењем дисконта у складу са МРС 8 Рачуноводствене политике, промјене рачуноводствених процјена и грешке код МП и зависних предузећа. ***Носилац активности:*** ***Управа МХ"ЕРС" и управе ЗП*** ***Рок:*** ***31.12.2023. године***

4. Начело сталности пословања

НАЛАЗИ РЕВИЗИЈЕ	ПРЕПОРУКА
На основу извршених ревизија појединачних финансијских извјештаја зависних предузећа - чланица Мјешовитог Холдинга за годину која се завршава на дан 31. децембра 2022. године, идентификовали смо код већине ентитета (Матично предузеће а.д. Требиње, Електрокрајина а.д. Бања Лука, Електро-Бијељина а.д. Бијељина, Електродистрибуција а.д. Пале, Електро Херцеговина а.д. Требиње, Хидроелектрана на Требишњици а.д. Требиње, Хидроелектрана Бистрица д.о.о. Фоча и РиТЕ Угљевик а.д. Угљевик) значајно веће текуће обавеза у односу на текућа средства у укупној вриједности од 291.053 хиљада КМ. Појединачни финансијски извјештаји чланица Холдинга као и консолидовани финансијски извјештаји Холдинга наводе да су исти састављени у складу са начелом сталности пословања. На основу спроведених ревизија код горе наведених чланица, утврдили смо постојање оперативних губитака, неликвидност и потенцијалне одливе значајних средстава по основу ризика од губљења судских спорова. Ово су индикатори постојања потенцијалних проблема везаних за могућност нормалног одвијања оперативних активности у смислу сервисирања текућих обавеза кроз наплату потраживања у договореним роковима и износима	Руководства чланица и Холдинга морају предузети детаљније и свеобухватније мјере обезбјеђивања континуираних извора финансирања, којим би се обезбедило нормално и континуирано обављање оперативних активности чланица Холдинга и самог Холдинга.

ОДГОВОР РУКОВОДСТВА

Препорука се прихвата.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА

Управе ће континуирано вршити процјену ликвидности и обезбјеђивати изворе финансирања, којим би се обезбедило нормално и континуирано обављање оперативних активности Друштва и самог Холдинга.

Носилац активности: Управа МХ"ЕРС"МП и свих ЗП

Рок: ***Континуирано***

5. Готовина и готовински еквиваленти

НАЛАЗИ РЕВИЗИЈЕ	ПРЕПОРУКА
У току ревизије консолидованих финансијских извјештаја на дан и за годину која се завршава 31.12.2022. године, Холдинг је на дан 31. децембра 2022. године, исказао стање готовине и готовинског еквивалента у износу од 38.273 хиљада КМ. Наведени износ укључује и дио одобреног, а неповученог кредита код комерцијалних банака у износу од 12.509 хиљада КМ (Зависно друштво Хидроелектране на Требишњици а.д. Требиње). За исти износ по основу одобреног неповученог кредита, Холдинг је увећао дугорочне обавезе по кредитима. Наведено евидентирање неповученог дијела кредита, имало је за посљедицу прецјењивање позиције готовине и готовинског еквивалента, односно текућих средстава у износу од 12.509 хиљада КМ, и прецјењивање дугорочних кредита, односно дугорочних обавеза у истом износу.	Препорука Ревизора је да Холдинг изврши корекцију стања готовине и готовинског еквивалента, као и стање дугорочних кредита, а евидентирање обавеза по основу неповучених кредитних средстава изврши у складу са захтјевима МРС 1 Презентација финансијских извјештаја, односно у оквиру ванбилансне евиденције. Сва додатна појашњења Холдинг треба да објелодани у напомене уз појединачне и консолидоване финансијске извјештаје.

ОДГОВОР РУКОВОДСТВА

Препорука се прихвата.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА

Извршити корекције складу са захтјевима МРС 1. Преостали износ кредита на дан 31.12.2022. године водиће се кроз ванбилансну евиденцију и приликом сваког новог повлачења вршиће се укидање ванбилансне евиденције и задуживати текући рачун предузећа док ће обавезе по кредитима потрживати за исти износ. Корекције ће бити објављене у Напоменама.

Носилац активности: Управа ЗП ХЕ на Требишњици

Рок: ***31.12.2023.***

6. Залихе и дати аванси

НАЛАЗИ РЕВИЗИЈЕ	ПРЕПОРУКА
Током обављања ревизије, констатовано је да су залихе на дан 31. децембра 2022. године исказане у износу од 126.889 хиљада КМ. Ревизорским поступцима утврђено је да залихе материјала и резервних дијелова, код већег броја зависних предузећа имају изузетно низак коефицијент обрта. Холдинг није вршио вредновање, односно усклађивање вриједности залиха у складу са параграфом 9 МРС 2 – Залихе.	Препорука ревизора је да сва Зависна предузећа на дан састављања појединачних финансијских извјештаја изврше процјену надокнадивост залиха материјала и резервних дијелова у складу са захтјевима МРС 2 „Залихе" и да на основу извршене анализе и процјене евидентирају губитке по основу усклађивања вриједности залиха.

ОДГОВОР РУКОВОДСТВА

Препорука се прихвата.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА

Формирати комисије које ће извршити ванредан попис залиха и одредити виталност употребе поменутих залиха и могућност њиховог даљег коришћења, те извршити усклађивање вриједности залиха у складу са захтјевима МРС 2.

Носилац активности: Управе зависних предузећа

Рок: ***28.02.2024.***

7. Књижење ефеката и исправке грешака из ранијег периода

НАЛАЗИ РЕВИЗИЈЕ	ПРЕПОРУКА
У току ревизије констатовано је да је Зависно предузеће Електро Бијељина а.д. Бијељина у току 2022. године извршило исправку грешке из ранијег периода у износу од 1.732 хиљаде КМ кроз текући период, смањењем нераспоређене добити. Наведено евидентирање исправке грешака из ранијег периода није у складу са захтјевима МРС 8 Рачуноводствене политике, промјене рачуноводствених процјена и грешке.	Препорука ревизора је да Друштво књижење ефеката исправке грешака врши у складу са захтјевима МРС 8 Рачуноводствене политике, промјене рачуноводствених процјена и грешке.

ОДГОВОР РУКОВОДСТВА
Препорука се прихвата.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА
Књижења ће се вршити у складу са усвојеним рачуноводственим политикама и Међународним рачуноводственим стандардима. *Носилац активности: Управа ЗП ЕД Бијељина* *Рок: 28.02.2024.*

8. Попуњавање финансијских извјештаја – (ЕД Бијељина)

НАЛАЗИ РЕВИЗИЈЕ	ПРЕПОРУКА
Током ревизије констатовано је да консолидовани финансијски извјештаји нису усаглашени са финансијским евиденцијама прије сачињавања појединачних и консолидованих финансијских извјештаја.	Препорука Ревизора је да Друштва приликом састављања финансијских извјештаја изврши формалну и суштинску контролу података који се уносе у појединачне и консолидоване финансијске извјештаје.

ОДГОВОР РУКОВОДСТВА
Препорука се прихвата.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА
Приликом састављања финанисјких извјештаја Предузеће ће вршити формалну и суштинску контролу података.
Носилац активности: Управа ЗП ЕД Бијељина
Рок: 28.02.2024.

ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ

5. Свеобухватна анализа информационог система

ЗНАЧАЈНИ ДОГАЂАЈИ У ИНФОРМАЦИОНОМ СИСТЕМУ

Током претходне године издвојени су сљедећи значајни догађаји у информационом систему свих чланица Холдинга:

- Успостављена је нова организација пословних процеса, посебно за формиране нове дирекције: Дирекцију за тржишно снабдијевање и Дирекцију за јавно снабдијевање (централизација дијела пословних процеса).
- Имплементиран је Софтвер за интегрисани билинг рачуна у свим чланицама Холдинга са изузетком Електро-Бијељине, гдје је у току поступак јавне набавке ОБС билинг.
- Двије новоформиране дирекције су успоставиле стабилан рад.
- У току је пројекат унапређења корпоративне безбједности за цијелу ЕРС, који се води од стране Матичног предузећа.
- Све производне и дистрибутивне SCADA мреже су ефективно раздвојене /сегментиране од остатка корпоративне мреже, осим у изузецима који су дио налаза ревизије.
- Друштво је проширило имплементације софтвера за резервне копије Veeam у зависним предузећима, при чему мањи дио предузећа и даље не користи софтвер за резервне копије.
- Организациона јединица Контакт центар у Бијељина функционише као дио Дирекције за јавно снабдијевање Матичног предузећа. У току је набавка софтвера за потребе Контакт центра.

Негативна запажања су:

- Друштво не проводи снимање сесија администрације ванјских компанија које су уговорно ангажоване у ЕРС, чиме се излаже ризицима повезним са неадекватном превенцијом упада и ограничењима управљања у случајевима безбједносних криза.
- Софтвер за резервне копије података није имплементиран у свим зависним друштвима.
- Постоји више локацијски дистрибуираних система који и даље нису у домену, чиме нису наметнуте јединствене безбједносне поставке за све рачунарске мреже и системе.
- Холдинг нема јединствене инфраструктурне стандарде. Софтверски системи су већим дијелом стандардизовани, иако се користе различите архитектуре система за дистрибутивни софтвер (Електродистрибуција Пале, Матично предузеће, Електрокрајина, Електро-Херцеговина) и интерни развој (Електро Добој).
- За критично важне системе је успостављено логовање приступа у складу са добрим праксама, али није успостављена двофакторска аутентификација. Друштво је припремило пројекат имплементације Двофакторске аутентификације, за који се очекује процедура набавке.
- Евиденција захтјева корисника се прима и евидентира софтверским путем само за ЕРП систем, при чему процес није конзистентно имплементиран за све врсте корисничких захтјева.

На нивоу зависник предузећа додатне значајне измјене су:

- Унапријеђено је наметање безбједносних политика на доменима у више предузећа. Шифре за доменске налоге се мијењају на редовној основи.
- Настављена је имплементација система безбједности према стандарду ISO27001 у неким зависним предузећима. Очекује се да овај систем управљања заживи и у Матичном предузећу и осталим зависним предузећима.
- Менаџмент сервер за ChekPoint рјешење за управљање мрежом је такође подигнут на виртуелној инфраструктури (ХЕТ, РИТЕ Гацко). Cisco Identity протокол којом се штити мрежа и изнутра и вани. Двофакторска аутентификација се тренутно не користи за све приступе. За приступ извана се користи искључиво VPN приступ, који је значајно проширен коришћењем током ковид кризе. Радовно се ажурирају дефиниције за повезане ватрозидне уређаје. Користе се и унапријеђене верзије мултиплексера, додатно се користи разервна комуникацијска мрежа. Мрежа у већини компанија развија и приоритетно користи оптичку инфраструктуру.
- Провјерени SCADA системи су већином у засебној мрежи, осим VPN везе према главном диспечерском центру Електропривреде РС. Ова веза се користи за терминирање искључиво унутрашњег саобраћаја.
- SAP системи и ИТ центри су додатно заштићени издвајањем у засебне и разумно осигуране виртуелне мреже.

НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	ПРЕПОРУКА, ПОБОЉШАЊА И СТАТУС
Унутар информационог система извршена су велика улагања у имовину. Претходне финансијске ревизије биле су фокусиране на критичне контроле, које су од интереса за ревизију финансијских извјештаја Холдинга. Није успостављен стратегијски план и циљеви развоја информационог система. **Ризик** Без детаљне анализе ИТ процеса и њихове усклађености и оперативне ефикасности, пословно руководство нема могућност потпуног сагледавања и праћења критичних промјена и стратегијског балансирања у подручју критичне инфраструктуре, сајбер безбједности и развоја пословних процеса/софтверске подршке.	Препорука је да Холдинг у наредном периоду планира анализу информационог система ради прегледа оперативног и стратегијског статуса кључних ИТ процеса. **Статус препоруке у 2021. години** Препорука није проведена. Због ове чињенице, ниво ризика налаза се процјењује као врло висок ризик. Свеобухватна анализа ИТ процеса и консолидација ИТ стратегије представља критичну компоненту трошковно ефикасног планирања. **Статус препоруке у 2022. години** Препорука није проведена. Постоји предметна ставка у плану набавке (Привремени оперативни план набавки за 2023. годину), али она није у току

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА
Детаљна анализа ИТ процеса ће се извршити током 2023 године. **Носилац активности: шеф Службе за ТИС** **Рок: 31.12.2023.**

9. Контрола приступа добављача (налаз из 2020.г.)

НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	ПРЕПОРУКА И СТАТУС
У току ревизије уочено је да већина добављача користи VPN приступ код администрације различитих система, при чему се надзор приступа остварује на елементарном нивоу, уз успостављање и контролу системских записа комуникационе опреме. **Ризик** Не постоје детаљнији подаци о акцијама проведеним у систему након успостављања приступа на рачунарску мрежу од стране добављача. У случају компромитације добављача, постоји проблем са повјерењем у проведене сигурносне мјере.	Размотрити набавку софтвера за надзор приступа добављача на нивоу снимања сесија администрације, који може обезбиједити брзу реакцију на инциденте и форензички квалитетне податке у случају упада у информациони систем. **Статус препоруке у 2021. години** Препорука није проведена. **Статус препоруке у 2022. години** Препорука није проведена

ОДГОВОР РУКОВОДСТВА
У току је имплементација рјешења.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА
-

10. Консолидација инфраструктурних стандарда информационог система (налаз из 2021.г.)

НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	ПРЕПОРУКА И СТАТУС
Унутар информационог система заступљени су системи различитих произвођача, чија набавка и имплементација није водила рачуна о дугорочном поравнању и консолидацији рјешења и добављача унутар ЕРС. **Ризик** Увећање трошкова кроз одвојене набавке, изостанак координације или набавка технички неспојивих рјешења. Лошији услови набавке и одржавања код глобалних и локалних добављача.	Препоручује се да Холдинг у наредном периоду предложи јединствене стандарде или препоруке за мрежну, серверску и SCADA инфраструктуру. **Статус препоруке у 2022. години** Препорука је већим дијелом проведена, због успостављања координације набавке. Са друге стране, потпуна консолидација рјешења због кризе ланаца снабдијевања за ИТ не мора бити најбољи избор.

ОДГОВОР РУКОВОДСТВА

Поред процеса координације, потребно је успоставити заједнички план са зависним предузећима, постоји велики број различитих произвођача и система јавних набавки, чак и унутар истих предузећа.

Ова препорука је тешко изведива, због ограничених надлежности Матичног предузећа.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА

-

11. План континуитета пословања - BCP (налаз из 2021.г.)

НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	ПРЕПОРУКА И СТАТУС
Идентификовали смо да Холдинг нема План континуитета пословања (Business Continuity Plan - BCP). Неки дијелови BCP се спомињу у ИТ процедурама као што је Опоравак од хаварије, али недостају кључне тачке. Нпр, када и како се покреће управљање кризним ситуацијама, листа особа које су задужене за управљање кризним ситуацијама са њиховим контакт подацима. Поред тога, постоји локација за опоравак од катастрофе (Disaster Recovery - DR), али нису достављени докази (редовни извјештаји) у вези са спроведеним тестом функционалности DR локације или опоравком пословних процеса. Безбједносни дизајн плана опоравка није усаглашен са новим сајбер ризицима. Ризик Тамо гдје недостаје План континуитета пословања и План опоравка од катастрофа није добро документован, те постоји ризик да се критични пословни процеси не могу заштитити од посљедица великог квара информационих система или ако дође до катастрофе. Ако се не спроведу годишње провјере локација DR-а, постоји ризик да ће се критичне информације за пословни субјект изгубити у случају великог неуспјеха ИС или катастрофе. Како препорука није ријешена у више узастопних година, ниво ризика се увећава на врло висок ризик.	Препоручујемо Холдингу да креира План континуитета пословања који укључује опоравак информационог система у случају катастрофе. BCP треба развијати и одржавати. Такође би требало да се заснива на процјени ризика и анализи пословних утицаја (BIA) како би се утврдила критичност система и процеса. Што се тиче локације DR, треба провести тестирање функционалности (најмање једном годишње) заједно са извјештајем о резултатима тестирања. Потребно је преиспитати дизајн процеса опоравка на начин да укључи додатне комбинације мјера заштите за новије пријетње (више копија, копије података на резервној локацији, употребу енкрипције и офлајн копије података, на примјер 3-2-1 дизајн)

ОДГОВОР РУКОВОДСТВА

Усвојен је План набавку у коме се налазила ставка избора консултанта за израду Плана континуитета. Нико се није јавио на предметну јавну набавку, план је да буде поновљена.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА

Спровести планирану набавку.

Носилац активности: шеф Службе за ТИС

Рок: 31.12.2023.

12. Примјена тикетног система (налаз из 2021.г.)	
НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	**ПРЕПОРУКА И СТАТУС**
Размотрити трошкове лиценцирања ЕРП система (попут РиТЕ Гацко) или специјализована софтверска рјешења за софтверско евидентирање и праћење важних ИТ задатака и управљање промјенама.	

ОДГОВОР РУКОВОДСТВА
Примјена је повећана али и даље није свеобухватна, те предузеће разматра опције која су повезана са контакт центрима и подршком.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА
Биће размотрена набавка ЕРП система. **Носилац активности: шеф Службе за ТИС** **Рок: 31.12.2023.**

13. Замјена застарјелих SCADA система (налаз из 2021.г.) – РиТЕ Гацко

НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	ПРЕПОРУКА И СТАТУС
Друштво користи дио SCADA система старије генерације за које није замијењен системски софтвер, те је повећана рањивост ових система на рачунарске пријетње. Систем користи хардвер који није обновљен (два ормара) у дужем временском периоду, иако се замјена планира такође дужи низ година. Одгађање замјене представља и безбједносни ризик, због употребе старијих верзија хардвера и системског софтвера. **РИЗИК** Већа изложеност експлоатацији познатих рањивости која постоје у SCADA системима старије генерације.	Размотрити убрзање имплементације раније предложене замјене дијела производних SCADA система **Статус препоруке у 2022. години** Препорука је ријешена. У току је ремонт који укључује замјену предметних система.

ОДГОВОР РУКОВОДСТВА

Очекујемо замјену ових система у току планираног ремонта.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА

-

14. Обезбјеђење ресурса за едукацију (налаз из 2021.г.) – РиТЕ Гацко и ЕД Бијељина

НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	ПРЕПОРУКА И СТАТУС
Предузеће не реализују планирана буџетска средства за потребе стручне едукације. **РИЗИК** Неодржавање потребног нивоа техничких и оперативних вјештина стручног кадра предузећа представља оперативни ризик.	Размотрити редовно годишње одржавање потребних стручних едукација. **Статус препоруке у 2022. години** Препорука није рјешена.

ОДГОВОР РУКОВОДСТВА

Размотрићемо редовно годишње одржавање потребних стручних едукација.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА

Повећати број стручних едукација. Организовање едукација у оквиру предузећа и упућивање радника на стручне семинаре и обуке.

Мотивисати раднике да се више ангажују у погледу редовног похађања едукација и стручног усавршавања кроз online обуке које не изискују путовања и боравак ван мјеста рада.

Носилац активности: Извршни директори, Руководиоци радних јединица, сектора и самосталних служби

Рок: Континуирано

15. Сегментација мреже и изолација SCADA система (налаз из 2021.г.) – ХЕ на Требишњици

НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	ПРЕПОРУКА И СТАТУС
Не постоји одговарајућа имплементација одвајања SCADA система од корпоративне мреже опште намјене. Дио имплементације користи мрежне уређаје који су дио корпоративне инфраструктуре. **РИЗИК** Постоји велики оперативни ризик од напада на SCADA мреже и координиране хакерске нападе, опасност од ширења утицаја напада на стабилност енергетске мреже државе.	Да би се отклонили описани ризици, потребно је покренути поступак издвајања инфраструктуре SCADA система у потпуно независну функционалну мрежу, безбједан дизајн и избјегавање изложености хакерским нападима. **Статус препоруке у 2022. години** **Препорука је реализована.** Дио нових система заштите је имплементиран или је у завршној фази реализације. Измјенама су уведене и нове мјере заштите предметног мрежног саобраћаја.

ОДГОВОР РУКОВОДСТВА
Препорука је реализована. Уврстићемо доградњу рачунарских мрежа у План за 2023. годину

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА
-

16. Коришћење старих оперативних система на рачунарима и серверима (налаз из 2021.г.) – ХЕ на Врбасу

НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	ПРЕПОРУКА И СТАТУС
Постоји одређен број застарјеле рачунарске опреме који користе застарјеле верзије оперативних система (MS Windows XP, MS Windows 7). **РИЗИК** Постоји значајан оперативни ризик и ризик искоришћавања слабости у неподржаним верзијама застарјелих оперативних система код сајбер напада.	Предузеће треба да замијени Windows XP/Windows 7 са новијим и подржаним верзијама. Windows Server 2003 треба бити замијењен са новијим и од произвођача подржаним верзијама системског софтвера. Статус препоруке у 2022. години Препорука је великом већином реализована

ОДГОВОР РУКОВОДСТВА
У току је набавка серверске инфраструктуре и неопходних уређаја за складиштење података. Очекује се потписивање уговора и испорука недостајуће рачунарске опреме.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА

17. Софтверска подршка изради резевних копија (налаз из 2020.г.) – ХЕ на Врбасу

НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	ПРЕПОРУКА И СТАТУС
У току ревизије уочено је да већина предузећа користи софтверску подршку за израду резервних колија система, али ове мјере нису конзистентно проведене на нивоу цијелог Холдинга/предузећа. **РИЗИК** Безбједносне мјере су имплементиране на различит начин, нису успостављени оквири за управљање ризицима у дијелу анализе утицаја код опоравка различитих група података.	Размотрити централизовану набавку софтвера за резервне копије и коришћење јединствених стандарда за чување резервних копија података за све компаније унутар Холдинга/предузећа. **Статус препорука у 2022. години:** Препорука је реализована.

ОДГОВОР РУКОВОДСТВА
Препорука је реализована

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА
-

18. Имплементација доменских политика (налаз из 2021.г.) – ХЕ на Врбасу

НАЛАЗИ РЕВИЗИЈЕ И РИЗИК	ПРЕПОРУКА И СТАТУС
Не постоји одговарајућа имплементација доменске администрације безбједносних политика у рачунарској мрежи Предузећа. **РИЗИК** Постоји значајан оперативни ризик и ризик искоришћавања слабости у администрацији система и безбједносних политика.	Предузеће треба да имплементира доменско намјетање безбједносних политика за све клијенте у рачунарској мрежи Предузећа. **Одговори руководства за 2021. годину:** У току је набавка серверске инфраструктуре која ће бити искоришћена за AD имплементацију у рачунарској мрежи Предузећа. **Статус препоруке у 2022. години:** Препорука није реализована.

ОДГОВОР РУКОВОДСТВА

За ове потребе ће се набавити одређена серверска инфраструктура.

МЈЕРА ЗА ОТКЛАЊАЊЕ НЕДОСТАТАКА

Донијети одлуке о примјени доменских политика и набавати одговарајућу серверску инфраструктуру.

Носилац активности: Управа Предузећа и Информатичка служба

Рок: 2024. година