Канцеларија за дуално образовање и Национални оквир квалификација

Акт о процени ризика

Београд, јун 2026.

Садржај

АКТ О ПРОЦЕНИ РИЗИКА

У циљу унапређења информационог система у оквиру Канцеларије за дуално образовање и национални оквир квалификација, примењена је методологија процене ризика из *Правилника о општој методологији за процену ризика у информационо-комуникационим системима од посебног значаја* (у даљем тексту: правилник) за сваки информациони ресурс од значаја у оквиру посматраног информационог система. Општа методологија за процену ризика у приоритетним и важним ИКТ системима од посебног значаја представља оквир за спровођење обавезе процене ризика прописане Законом о информационој безбедности („Службени гласник РС“, број 91/25, у даљем тексту: ЗИБ). У складу са Законом оператери ИКТ система од посебног значаја дужни су да донесу Акт о процени ризика за ИКТ системе. Овај процес подразумева идентификацију претњи и рањивости која се заснива на Каталогу претњи из Прилога 2 правилника, као и квантификацију и класификацију затеченог ризика, у складу са законом, узимајући у обзир величину и значај оператора, вероватноћу и озбиљност безбедносних инцидената, као и њихов потенцијални друштвени и економски утицај. Ризик се у контексту информационе безбедности може моделовати као комбинација последица по информациони ресурс након безбедносног догађаја, и вероватноће да се тај догађај реализује. Идентификација ризика почиње идентификацијом информационих добара или ресурса, пословних процеса и процедура који су неопходни за несметано и континуирано пословање организације.

Коришћени појмови

У методологији се користе појмови из области информационе безбедности, ИКТ система и процеса управљања ризицима. У наставку су наведени појмови и њихова значења онако како су дефинисана у правилнику и како су коришћена приликом израде овог акта:

Појмови	Значење
Анализа ризика	Процес разумевања природе ризика и утврђивања нивоа ризика. Представља основу за вредновање ризика и доношење одлука о третману ризика.
Вероватноћа догађаја	Шанса да се одређени догађај или претња оствари.
Власник ресурса	Особа која је одговорна за ресурсе.
Власник ризика	Особа која је одговорна и овлашћена да управља ризиком.
Вредност ризика	Комбинација негативног утицаја и вероватноће појаве ризика, односно вероватноће догађања.
Догађај (event)	Појава или промена одређеног скупа околности која може имати значај за безбедност или пословање.
Идентификација ризика	Процес препознавања и описивања ризика.

Инцидент	Сваки догађај који угрожава расположивост, интегритет, аутентичност, непорецивост или поверљивост података који се чувају, преносе или обрађују или услуге које се пружају, односно које су доступне путем ИКТ система.
Инхерентни ризик	Вредност ризика пре примене мера заштите.
Информисана одлука (Informed decision)	Одлука о поступању са ризиком коју доноси орган управљања оператора ИКТ система од посебног значаја на основу документованих резултата процене ризика, узимајући у обзир идентификоване претње, процењени утицај и вероватноћу, расположиве мере заштите и пословни контекст.
Мере заштите	Техничке, организационе, административне и физичке мере за управљање безбедносним ризицима ИКТ система.
Поступање са ризиком	Третирање ризика ради смањења, елиминације или превенције негативних последица.
Поверљивост (confidentiality)	Својство којим се осигурава да су информације и функције ИКТ система доступне само овлашћеним лицима.
Преостали ризик (residual risk)	Ризик који преостаје након поступања са ризиком, односно након примене мера заштите.
Прихватање ризика	Свесна одлука о прихватању одређеног ризика.
Претња	Свака околност, догађај или радња која може да угрози, поремети или на други начин штетно утиче на ИКТ систем, кориснике система и друга лица са јасном вероватноћом настајања штете у случају да изостане реакција.
Процена ризика	Процена ризика, у смислу ове методологије, је систематски процес идентификације, анализе и вредновања ризика који могу утицати на ресурсе оператора ИКТ система од посебног значаја, са циљем да се обезбеде информисане одлуке о поступању са тим ризицима. Процена ризика обухвата и поступање са ризиком и праћење ризика као саставне фазе целокупног циклуса управљања ризицима информационе безбедности.
Расположивост (availability)	Један од три кључна атрибута информационе безбедности, својство којим се осигурава доступност и употребљивост ИКТ система на захтев овлашћеног субјекта или процеса онда када им је потребан.
Ресурси (asset)	Све што има вредност за оператора ИКТ система од посебног значаја, укључујући податке, хардвер, софтвер, локације и људске ресурсе.
Ризик	Функција негативног утицаја специфичне последице и вероватноће њеног настанка.
Управљање ризицима	Свеобухватан процес усмерен на контролу ризика унутар ИКТ система од посебног значаја.
Утицај (impact)	Степен негативних последица по остваривање пословних циљева у случају реализације ризика.
Фреквенција	Мера учесталости појаве одређеног догађаја.

Опсег процене

Овај текст је формулисан у складу са захтевима за операторе ИКТ система од посебног значаја (према ЗИБ Републике Србије) и садржи податке о локацијама и ресурсима ИКТ система Канцеларије за дуално образовање и национални оквир квалификација. Оператор ИКТ система од посебног значаја је дужан да донесе акт о процени ризика за ИКТ систем којим управља. Актом о процени ризика се врши процена ризика за ИКТ систем од посебног значаја с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај.

Дефиниција опсега и контекста процене ризика

Дефинисањем опсега и контекста успостављају се границе унутар којих се спроводи процена ризика, чиме се осигурава да сви критични ресурси и пословни процеси клијента буду адекватно заштићени.

1. Надлежност и обухват

Оператор ИКТ система од посебног значаја управља инфраструктуром која се простире на више локација. Канцеларија за дуално образовање и национални оквир квалификација планира развој и спроводи мере и активности у области дуалног образовања у складу са усвојеним стратешким документима, међународним конвенцијама и другим актима. Канцеларија припрема стручне основе и израђује законе и подзаконске акте из дуалног образовања у средњем стручном образовању, дуалног модела студија у високом образовању, каријерног вођења и саветовања , као и Националног оквира квалификација Републике Србије (НОКС). Део надлежности Канцеларије је праћење примене закона и прописа из ових области, као и процена ефеката увођења дуалног образовања у средњем стручном образовању и високом образовању и НОКС-а у складу са стратешким документима. Опсег процене обухвата све елементе ИКТ система који подржавају континуитет пословања и заштиту података, са посебним фокусом на:

- Административне центре: Локације у Немањиној 22-26 и Јурија Гагарина 76.
- Критичну инфраструктуру: Сервери и виртуелна окружења смештени у Државном Дата Центру (ДДЦ) у Крагујевцу.
- Мрежна чворишта: Инфраструктура у Палати Србија.

2. Заинтересоване стране и очекивања

У оквиру анализе контекста идентификоване су кључне стране чија су очекивања пресудна за дефинисање нивоа безбедности:

- Корисници и запослени: Очекују сталну доступност сервиса и интегритет података.
- Регулаторна тела (Министарство, РАТЕЛ): Захтевају потпуну усклађеност са законском регулативом и стандардима информационе безбедности.
- Екстерни партнери (ДДЦ Крагујевац, Телеком Србија): Очекују дефинисане нивое одговорности у управљању дељеном инфраструктуром.

3. Интерни и екстерни изазови

Анализа контекста препознаје специфичне изазове који могу утицати на безбедносни профил:

- Екстерни изазови: Велика зависност од треће стране (ДДЦ Крагујевац) за критичне сервисе и виртуелну инфраструктуру, као и потенцијалне претње мрежној стабилности на локацији Палата Србија.
- Интерни изазови: Управљање хардверским ресурсима (радне станице и мрежа) на физички раздвојеним локацијама у Београду, као и континуирана обука запослених (ресурс ИД03) који представљају прву линију одбране система.

4. Физички и логички опсег ресурса

Процена ризика се спроводи над следећим категоријама ресурса према важећем регистру:

Категорија ресурса	Кључни елементи	Локације
Хардвер	Радне станице и локална мрежна опрема (**ID01**, **ID02, ID07, ID08**)	Београд (Немањина, Ј. Гагарина)
ИКТ Услуге	Виртуелна инфраструктура и системски мрежни ресурси (**ID06**)	ДДЦ Крагујевац
Људски ресурси	Сви запослени са приступом ИКТ систему (**ID03**)	Београд (Немањина, Ј. Гагарина)
Локације и простори	Пословне просторије, канцеларије и серверске сале (**ID04**, **ID05**)	Београд (Немањина, Ј. Гагарина)

5. Критеријуми за процену и организација

Критеријуми за процену ризика дефинисани су кроз нивое утицаја на поверљивост, интегритет и доступност података. За потребе овог процеса, постоји тим за управљање ризицима, састављен од власника ресурса (власници за ИД01-ИД08) и стручњака за информациону безбедност.

Овај оквир обезбеђује да резултати анализе буду доследни, упоредиви и поуздани, пружајући основу за доношење одлука о третману ризика и даљим инвестицијама у безбедносне контроле.

Регистар ресурса

Прва фаза процеса процене ризика подразумева идентификацију информационих ресурса који су од важности у ИКТ систему, пре свега оних ресурса који се користе у оквиру критичних пословних активности и који имају вредност за оператора ИКТ система од посебног значаја. Поред овога, сваком ресурсу додељен је власник. Приликом идентификације ресурса неопходно је узети у обзир да се ИКТ систем не своди искључиво на хардверске и софтверске компоненте, већ обухвата шири спектар ресурса, укључујући локације, хардвер, софтвер, запослене, информације и треће стране. Идентификација ресурса коју је потребно заштити и процена њихове вредности (у смислу утицаја који ће оператор ИКТ система од посебног значаја претрпети у случају инцидента) су од кључног значаја приликом анализе ризика. Сваки ИКТ систем може обухватити следеће категорије ресурса:

- Локације,
- Хардвер (обухвата и мрежне уређаје и електронску комуникациону инфраструктуру у смислу ЗИБ-а),
- Софтвер, укључујући, али не ограничавајући се на интерне апликације, базе података, лиценце и резервне копије других ресурса од важности,
- Финансијске извештаје,
- Запослене (по улогама), њихове компетенције, и корисничке налоге, као и привилегије налога,
- Информације – нематеријалну имовину, и
- Треће стране (добављаче, сараднике и партнере).

Резултат процеса идентификације ресурса је израда регистра ресурса (*Табела 1*), који оператор ИКТ система од посебног значаја прилагођава својим потребама и организационом контексту и најмање садржи следеће податке:

- Назив ресурса или јединствени идентификатор ресурса – име које ће се користити за то средство у оквиру анализе ризика,
- Власник – име или радно место одговорне особе за правилно управљање или коришћење средства,
- Категорија, и
- Локација ресурса.

ID Ресурса	Назив ресурса	Власник	Категорија	Локација
ID01	Радне станице	Лука Шемић	Хардвер	Немањина 22-26
ID02	Радне станице	Лука Шемић	Хардвер	Јурија Гагарина 76
ID03	Запослени	Лука Шемић	Запослени	Обе локације
ID04	Локације и просторије	Лука Шемић	Локације и просторије	Немањина 22-26
ID05	Локације и просторије	Лука Шемић	Локације и просторије	Јурија Гагарина 76
ID06	Виртуелна инфраструктура	Лука Шемић	ИКТ услуга	Државни Дата Центар
ID07	Мрежна инфраструктура	Лука Шемић	Хардвер	Немањина 22-26
ID08	Мрежна инфраструктура	Лука Шемић	Хардвер	Јурија Гагарина 76

Идентификација претњи

Наредни корак јесте идентификација рањивости сваког од евидентираних информационих ресурса, а затим и претњи које потенцијално могу да се искористе за неауторизовани приступ подацима (нарушавање начела *тајности*), измену постојећих података (нарушавање начела *интегритета*) или брисање података (нарушавање начела *доступности*). Идентификација претњи је процес који се спроводи након што су ИКТ подсистеми, пословни процеси и ресурси у опсегу процене ризика јасно дефинисани. Оператор ИКТ система од посебног значаја користи Каталог претњи информационе безбедности (у даљем тексту: Каталог претњи), који је саставни део ове методологије, као основни извор за идентификацију претњи. Каталог претњи обухвата следеће категорије претњи:

- природне непогоде,
- неауторизоване приступе одређеном систему или сервису,
- грешке и ненамерни пропусти,
- социјални инжењеринг,
- физичке претње,
- малициозни софтвер,
- индустријске претње, и
- претње повезане са услугама које се пружају операторима ИКТ система од посебног значаја, укључујући услуге рачунарства у облаку и услуге трећих лица.

Резултати идентификације претњи документују се кроз дефинисање уређених релација између ресурса и претњи из Каталога претњи информационе безбедности (*Табела 2*). Ове релације представљају основу за даљу анализу и вредновање ризика.

Ресурс	Претња
Радне станице - ID01	**1.1** Ватра **1.2** Вода **1.4** Природне катастрофе **2.2** Прекид енергетског напајања **2.4** Квар хардвера или софтвера **2.5** Квар комуникационих услуга **2.7** Деградација медијума **2.9** Пренос злонамерног софтвера применом преносивих носача података **3.1** Корисничке грешке **3.3** Грешке праћења (записи) **3.4** Грешке у конфигурацији **3.6** Ширење злонамерног софтвера (малвера) **3.7** Случајна измена података **3.9** Цурење података **3.10** Рањивост софтвера **3.11** Грешке у одржавању/ажурирању софтвера **3.12** Квар система због исцрпљености ресурса **3.19** Неадекватно планирање континуитета пословања **3.21** Грешке у процедурама резервних копија (Backup) **4.3** Маскирање идентитета **4.4** Злоупотреба права приступа **4.5** Злоупотреба ресурса **4.6** Ширење малвера **4.7** Неовлашћен приступ **4.8** Анализа саобраћаја **4.10** Намерна измена информација **4.11** Уништавање информација
Радне станице - ID02	**1.1** Ватра **1.2** Вода **1.4** Природне катастрофе **2.2** Прекид енергетског напајања **2.4** Квар хардвера или софтвера **2.5** Квар комуникационих услуга **2.7** Деградација медијума **2.9** Пренос злонамерног софтвера применом преносивих носача података **3.1** Корисничке грешке **3.3** Грешке праћења (записи) **3.4** Грешке у конфигурацији **3.6** Ширење злонамерног софтвера (малвера) **3.7** Случајна измена података **3.9** Цурење података **3.10** Рањивост софтвера **3.11** Грешке у одржавању/ажурирању софтвера **3.12** Квар система због исцрпљености ресурса **3.19** Неадекватно планирање континуитета пословања **3.21** Грешке у процедурама резервних копија (Backup) **4.3** Маскирање идентитета **4.4** Злоупотреба права приступа

	4.5 Злоупотреба ресурса **4.6** Ширење малвера **4.7** Неовлашћен приступ **4.8** Анализа саобраћаја **4.10** Намерна измена информација **4.11** Уништавање информација
Запослени - ID03	**2.9** Пренос злонамерног софтвера применом преносних носача података **3.7** Случајна измена података **3.9** Цурење података **3.14** Недостатак запослених **3.15** Недостатак свести и специфичних знања о информационој безбедности **4.10** Намерна измена информација **4.11** Уништавање информација **4.12** Откривање информација **4.19** Социјални инжењеринг
Локације и просторије – ID04	**1.1** Ватра **1.2** Вода **1.4** Природне катастрофе **2.2** Прекид енергетског напајања
Локације и просторије – ID05	**1.1** Ватра **1.2** Вода **1.4** Природне катастрофе **2.2** Прекид енергетског напајања
Виртуелна инфраструктура – ID06	**2.2** Прекид енергетског напајања **2.5** Квар комуникационих услуга **2.6** Прекид основних услуга које су предмет набавке или других услуга **4.15** Ускраћивање услуга **5.3** Грешке код изолације **5.4** Несигурно или неефикасно брисање података **5.8** Анализа инцидената и форензичка подршка
Мрежна инфраструктура – ID07	**1.1** Ватра **1.2** Вода **1.4** Природне катастрофе **2.2** Прекид енергетског напајања **2.4** Квар хардвера или софтвера **2.5** Квар комуникационих услуга **3.4** Грешке у конфигурацији **3.12** Квар система због исцрпљености ресурса
Мрежна инфраструктура – ID08	**1.1** Ватра **1.2** Вода **1.4** Природне катастрофе **2.2** Прекид енергетског напајања **2.4** Квар хардвера или софтвера **2.5** Квар комуникационих услуга **3.4** Грешке у конфигурацији **3.12** Квар система због исцрпљености ресурса

Процена вероватноће и утицаја

Анализа ризика је процес у оквиру којег се врши процена значаја идентификованих ризика кроз анализу утицаја и вероватноће догађања претњи, и представља централну фазу процеса управљања ризицима информационе безбедности. Анализа ризика представља основ за управљање ризицима и полазну тачку за дефинисање циљева информационе безбедности усмерених на заштиту ресурса оператора ИКТ система од посебног значаја, односно доношење одлука о приоритетима, избору мера заштите и поступању са идентификованим ризицима. Вероватноћа да претња искористи постојећу рањивост ИКТ система зависи од следећих фактора:

- Вредности ресурса нападачу, која је углавном, али не нужно увек, финансијска,
- Историје претходних напада,
- Ризика да нападач буде откривен током или након напада, без обзира на његову успешност,
- Сложености вектора напада,
- Мотивације нападача, која може бити финансијске или личне природе, и
- Алата и вештина неопходних да се напад изврши.

Концепт „нападача“ у контексту природних непогода или стохастичних грешака у раду система није применљив, док у случају физичких претњи, неауторизованог приступа систему или злоупотребе, „нападач“ мора бити присутан у неком облику. Процена ризика у области информационе безбедности заснива се на анализи комбинације два кључна фактора: утицаја (енг. „*impact*“) и вероватноће (енг. „*probability*“) догађања. Негативан утицај представља један од два основна фактора за одређивање вредности ризика у оквиру квалитативне анализе ризика. Квалитативна анализа ризика подразумева употребу субјективних описа попут „ниска вероватноћа“, „средња вероватноћа“, „веома висок утицај“ или „висока вероватноћа“ као индикатора вероватноће дешавања догађања или могућег утицаја догађаја по ИКТ систем. Под негативним утицајем подразумева се степен штете који може настати по ресурсе оператора ИКТ система од посебног значаја и повезане пословне процесе у случају реализације одређене претње. Ради једноставније и доследне процене, негативан утицај се вреднује коришћењем скале од 1 до 5, у складу са документом *„Interoperable EU Risk Management Toolbox“* (*Табела 3*).

Утицај	Вредност	Опис
Веома висок - катастрофалан	5	• Реализација претње изазива катастрофалне последице по пословање. • Цурење информација које могу угрозити опстанак оператора ИКТ система од посебног значаја. • Цурење података о личности великог обима или осетљивих категорија података које може изазвати значајну штету по права и слободе физичких лица. • Непоправљиви кварови или трајни прекиди у раду система. • Недоступност која захтева екстремне напоре за повратак функционалности или је трајна.

		• Озбиљан негативан утицај на репутацију или запослене уз значајну медијску пажњу. • Престанак свих услуга које пружа оператор ИКТ система од посебног значаја. • Законске санкције или велике новчане казне. • Последице су скоро неповратне или ненадокнадиве (нпр. смрт, немогућност рада).
Висок – критичан	4	• Реализација изазива значајне негативне последице по пословање. • Цурење информација које озбиљно угрожава интересе оператора ИКТ система од посебног значаја. • Цурење података о личности које угрожава права и слободе физичких лица и може резултовати новчаним казнама у складу са прописима о заштити података о личности. • Наставак недоступности услуга са значајним оперативним проблемима. • Пад угледа оператора ИКТ система од посебног значаја. • Финансијски губици или додатни трошкови због претње.
Средњи – просечан	3	• Реализација изазива умерен негативни ефекат по пословање. • Цурење информација које утичу на интересе оператора ИКТ система од посебног значаја. • Привремена штета угледу. • Изоловани инциденти са минималним утицајем. • Потенцијалне казне или мањи финансијски губици.
Низак - маргиналан	2	• Реализација претње има ограничен утицај на пословање. • Цурење информација које су штетне, али не угрожавају виталне интересе. • Недостатак доступности услуга само изазива неугодности. • Могућа медијска критика, али без значајних последица. • Мали губици који се лако надокнађују (нпр. изгубљено време).
Веома низак - занемарљив	1	• Реализација претње има незнатан или минималан утицај на пословање.

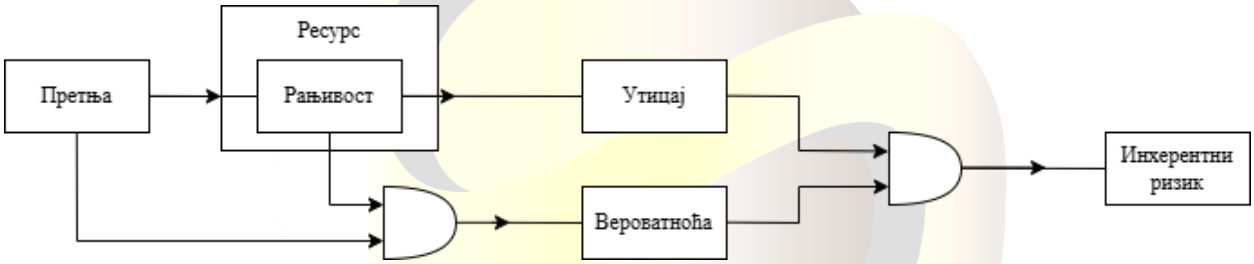
Вероватноћа догађања представља други кључни фактор за одређивање укупне вредности ризика у оквиру анализе ризика. Она означава процену шансе да се одређена претња оствари у контексту постојећих ИКТ система и пословних процеса оператора ИКТ система од посебног значаја. Слично као и код утицаја, и вероватноћа се вреднује коришћењем скале од 1 до 5, где вредности 1 представља малу вероватноћу реализације (тј. краткотрајне последице које немају већи ефекат на рад информационог система), а вредност 5 представља веома високу вероватноћу реализације (тј. озбиљне последице које могу довести до дуготрајног престанка пословних процеса, значајних директних или индиректних финансијских трошкова или репутационе штете) у складу са документом *„Interoperable EU Risk Management Toolbox“* (*Табела 4*).

Вероватноћа догађања	Вредност	Опис
Веома висока	5	Претња ће се скоро сигурно остварити због постојања рањивости које се могу искористити, а одговарајуће мере заштите не постоје. (*вероватноћа реализације у периоду од 0 до 90 дана*)
Висока	4	Претња ће се вероватно остварити, јер постоје рањивости које се могу искористити, а постојеће мере заштите су неефикасне или застареле. (*вероватноћа реализације у периоду од 90 до 180 дана*)
Средња	3	Претња се потенцијално може остварити због постојећих рањивости, иако постоје одређене мере заштите, које би могле бити ефикасније. (*вероватноћа реализације у периоду од 180 дана до 1 године*)
Ниска	2	Претња се вероватно неће остварити јер су све повезане рањивости покривене одговарајућим мерама заштите. (*вероватноћа реализације у периоду од 1 до 3 године*)
Веома ниска	1	Мало је вероватно да ће се претња остварити, будући да су све повезане рањивости ефикасно неутралисане мерама заштите.

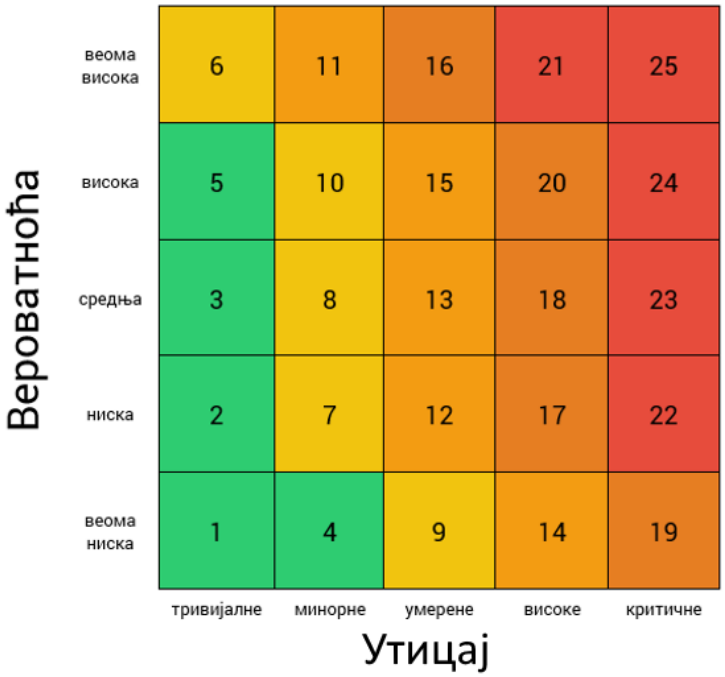
Матрица ризика

Ниво ризика сваке од идентификованих претњи је на нивоу свих критичних информационих ресурса израчунат као комбинација вероватноће и утицаја, затим и графички представљен употребом напредне матрице ризика која фаворизује претње са већом вероватноћом. Вредности приказане у матрици ризика и регистру ризика односе се на инхерентан ризик, односно ризик пре примене контролних мера заштите. Коришћена матрица ризика је подељена у пет региона, при чему сваки од њих одговара једној од следећих категоризација ризика према нивоу озбиљности:

1. Ниски ризици који се могу прихватити, али се свакако евидентирају,
2. Ризици који нису хитни, али могу захтевати примену накнадних мера,
3. Ризици који захтевају примену безбедносних мера,
4. Важни ризици који захтевају примену безбедносних мера, и
5. Ризици који захтевају хитну примену безбедносних мера



Фигура 1: Општи преглед процене ризика



Слика 1: Напредна матрица ризика

Поступање са ризиком

Поступање са ризиком обухвата активности и одлуке које оператор ИКТ система од посебног значаја предузима ради управљања идентификованим ризицима, са циљем њиховог смањења, контроле или прихватања. Поступање са ризиком подразумева спровођење активности или доношење одлука у вези са идентификованим ризицима, њиховим нивоом озбиљности и начином поступања. Процес укључује примену различитих стратегија и мера с циљем смањења вероватноће настанка ризика и ублажавања последица које ризици могу имати на безбедност информација.

Мере предлажу најадекватнији начин да се ниво ризика смањи, а то се може постићи кроз избегавање или потпуно елиминисање ризика, прихватање или толеранцију ризика, редукцију или модификацију ризика, и трансфер или дељење ризика. Прихватање ризика представља свесну одлуку оператора ИКТ система од посебног значаја да не предузима додатне мере за смањење или контролу одређених идентификованих ризика, већ да их задржи на одређеном, прихватљивом нивоу. Овај приступ подразумева да оператор ИКТ система од посебног значаја препознаје одређени степен изостанка безбедности или потенцијалну изложеност ризику, али оцењује да се ризик може толерисати у односу на постизање пословних циљева. Такође, прихватање ризика се примењује када су друге опције, попут преноса ризика или његовог потпуног избегавања, непрактичне или неекономичне. Трансфер или дељење ризика подразумева да оператор ИКТ система од посебног значаја дели управљање ризиком са трећом страном која је у могућности да га ефикасно контролише. То не значи да оператор ИКТ система од посебног значаја преноси одговорност за ризик, већ остаје примарно одговоран, али одређене активности у управљању ризиком се деле. Важно је напоменути да се може делити одговорност за управљање ризиком, али не и за последице које ризик може изазвати. Најчешћи начини пребацивања или дељења ризика су:

- **осигурање**: примењује се као мера за ублажавање последица ризика, којом се уговара накнада штете (најчешће у новчаном облику или кроз замену изгубљеног ресурса) у случају материјализације ризика, и
- **поверавање трећој страни** *(outsourcing)*: примењује се као организациона мера у оквиру које се одређене активности управљања или смањења ризика поверавају трећој страни, при чему одговорност за управљање ризиком остаје на оператору ИКТ система од посебног значаја.

Када идентификовани ризици имају превисоку вредност или када трошкови спровођења других мера превазилазе очекиване користи, може се донети одлука о потпуном избегавању ризика. То се постиже повлачењем из планираних или постојећих активности, изменом начина обављања активности или променом услова под којима се делатност спроводи. На пример, за ризике узроковане природом, једна од ефикасних мера може бити физичко пресељење објеката за обраду информација на локацију где је ризик елиминисан или под контролом. Међутим, у пракси, опција потпуног избегавања ризика ретко је примењива за операторе ИКТ система од посебног значаја.

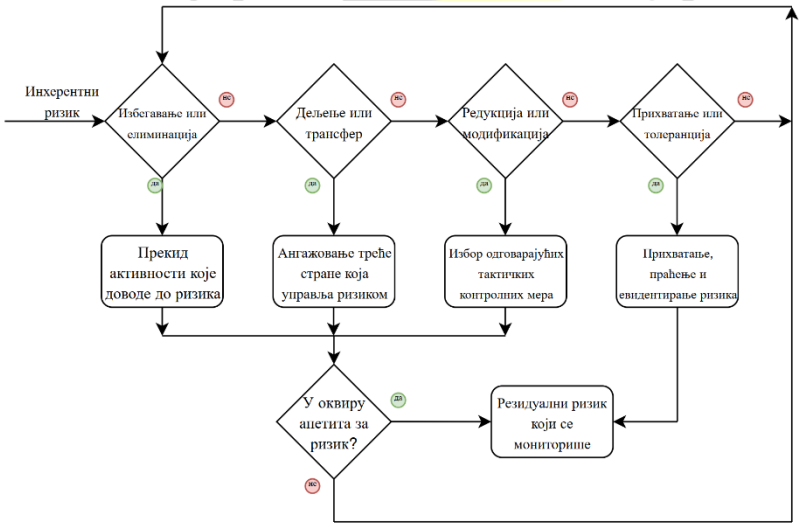
Управљање ризиком врши се увођењем, уклањањем или прилагођавањем мера заштите, тако да преостали (*residual*) ризик може бити процењен као прихватљив, у складу са критеријумом прихватљивости ризика. При одабиру мера заштите, важно је узети у обзир трошкове набавке, имплементације, администрације, рада, праћења и одржавања, у односу на вредност ресурса који се штити. Иако се модификација ризика често наводи као последња опција, она би у пракси

требало да буде најчешће примењивана, јер показује да оператор ИКТ система од посебног значаја свесно утиче на ниво ризика коришћењем мера заштите. Приликом примене ове стратегије, обавезно је израчунати преостали ризик након спровођења мера и евидентирати га у регистар ризика.

Оваква расподела представља стратешки слој управљања ризиком, и даље се може декомпоновати на тактички слој, којег чине мере детекције, превенције, дирекције и корекције, респективно. Стратешке контроле саме по себи не умањују инхерентан ризик, већ дефинишу жељени приступ за смањење ризика у најопштијем смислу. Тактичке контроле, попут стратешких, не утичу на смањење ризика, али за разлику од њих дефинишу конкретније активности за смањење ризика. Тактичке контроле се могу поделити на процедуралне, физичке и техничке. Процедуралне контроле дефинишу акције и жељено понашање корисника и техничког особља у свим околностима. Ове контроле инхерентно не смањују ни вероватноћу ни последице безбедносних догађаја осим ако их се корисници строго не држе. Наспрам њих, физичке контроле се тичу претњи у непосредном окружењу информационог ресурса, и као такве увек смањују или вероватноћу или последице (или оба ова фактора). Техничке контроле се директно односе на технологију која је основа за очекивани рад информационог система или добра. Могу бити имплементиране софтверски или хардверски, а најчешће на оба начина.

Прихватљиви ниво ризика

Жељени ниво ризика је у опсегу од 1-5, док је прихваћени апетит за ризик (“Risk Appetite”) 9. У контексту процене ризика, апетит за ризик је ниво ризика којег је предузеће спремно да прихвати или задржи у циљу испуњења дугорочних пословних циљева. Ова метрика представља општи став предузећа по питању предузимања ризика, док је толеранција ризика („Risk Tolerance“) нумерички индикатор прихватљивог ризика на нивоу конкретне претње или информационог ресурса у односу на апетит за ризиком. Ове метрике помажу при категоризацији ризика на оне који не превазилазе апетит за ризик и оне који захтевају примену додатних мера и контрола у циљу смањења резидуалног ризика на прихватљив ниво. Контролне мере се хијерархијски могу поделити на стратешке, тактичке и техничке мере, при чему су у наставку предлагане превасходно техничке мере.



Фигура 2: Процес стратешког управљања ризиком

Регистар ризика

Регистар ризика представља посебан документ који оператори ИКТ система од посебног значаја користе за праћење, документовање и управљање идентификованим ризицима. Регистар ризика представља пратећи документ Акту о процени ризика. Вредности ризика евидентиране у регистру ризика представљају инхерентни ризик, ризик процењен пре примене мера заштите и ризик процењен након примене контролних мера заштите – резидуалан ризик.

Регистар пружа свеобухватан преглед ризика, укључујући њихове карактеристике, вероватноћу, потенцијални утицај, стратегије поступања са ризиком и статус мера предузетих ради смањења или контроле ризика.

Регистар ризика садржи следеће елементе:

- Назив ресурса,
- Претњу,
- Вредности вероватноће догађања,
- Вредности утицаја,
- Вредности инхерентног ризика,
- Имплементиране мере заштите,
- Вредности резидуалног ризика,
- Поступање са ризиком у виду контролних мера, и
- Власника ризика.

Периодична ревизија

Регистар ризика се редовно ажурира, посебно након периодичне процене ризика, како би се осигурало да информације остану актуелне и релевантне. Оператор ИКТ система од посебног значаја је по Члану 11. Закона о информационој безбедности дужан да акт о процени ризика ревидира најмање једном годишње.