Република Србија

Државна ревизорска институција

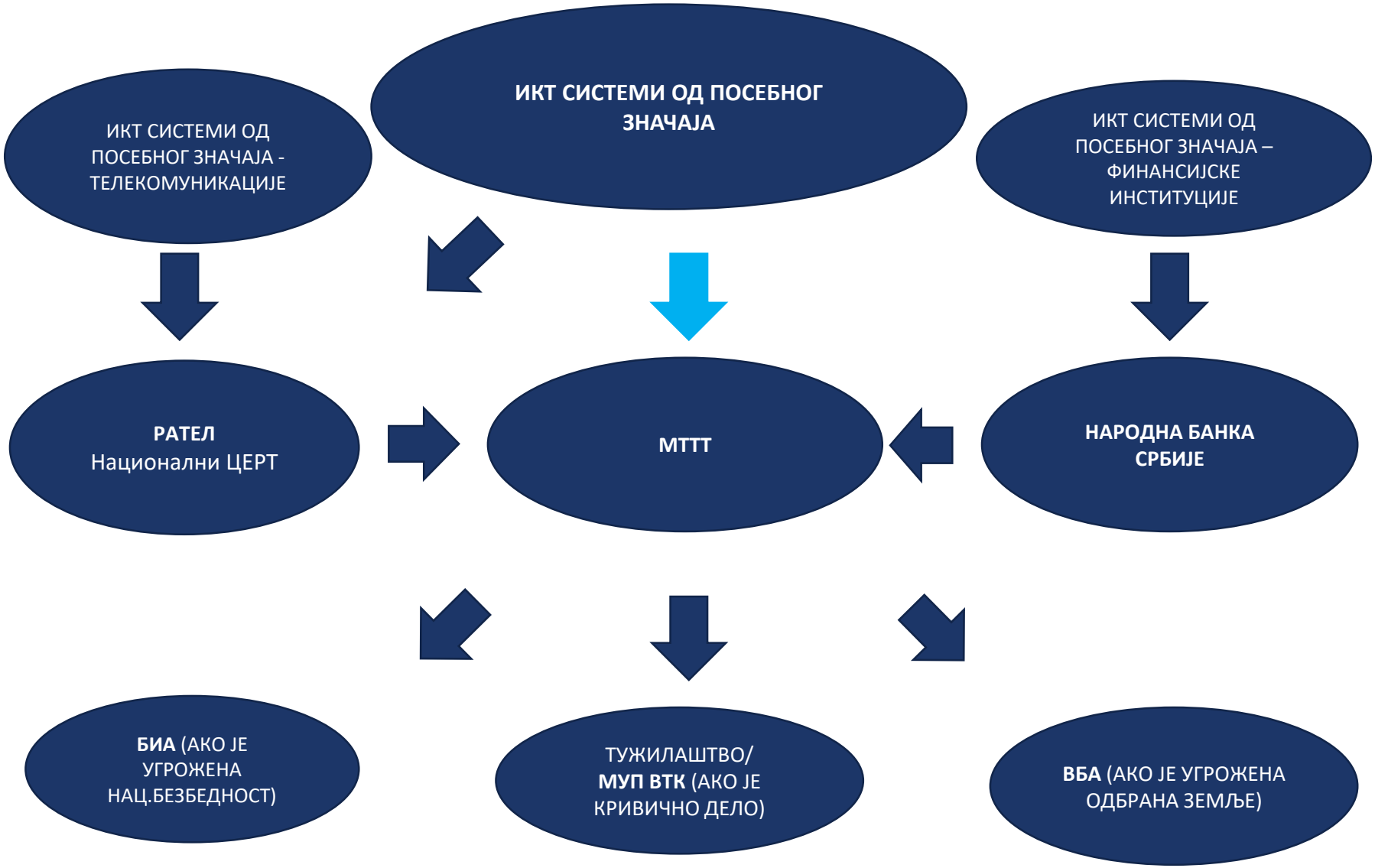
Ревизија сврсисходности пословања

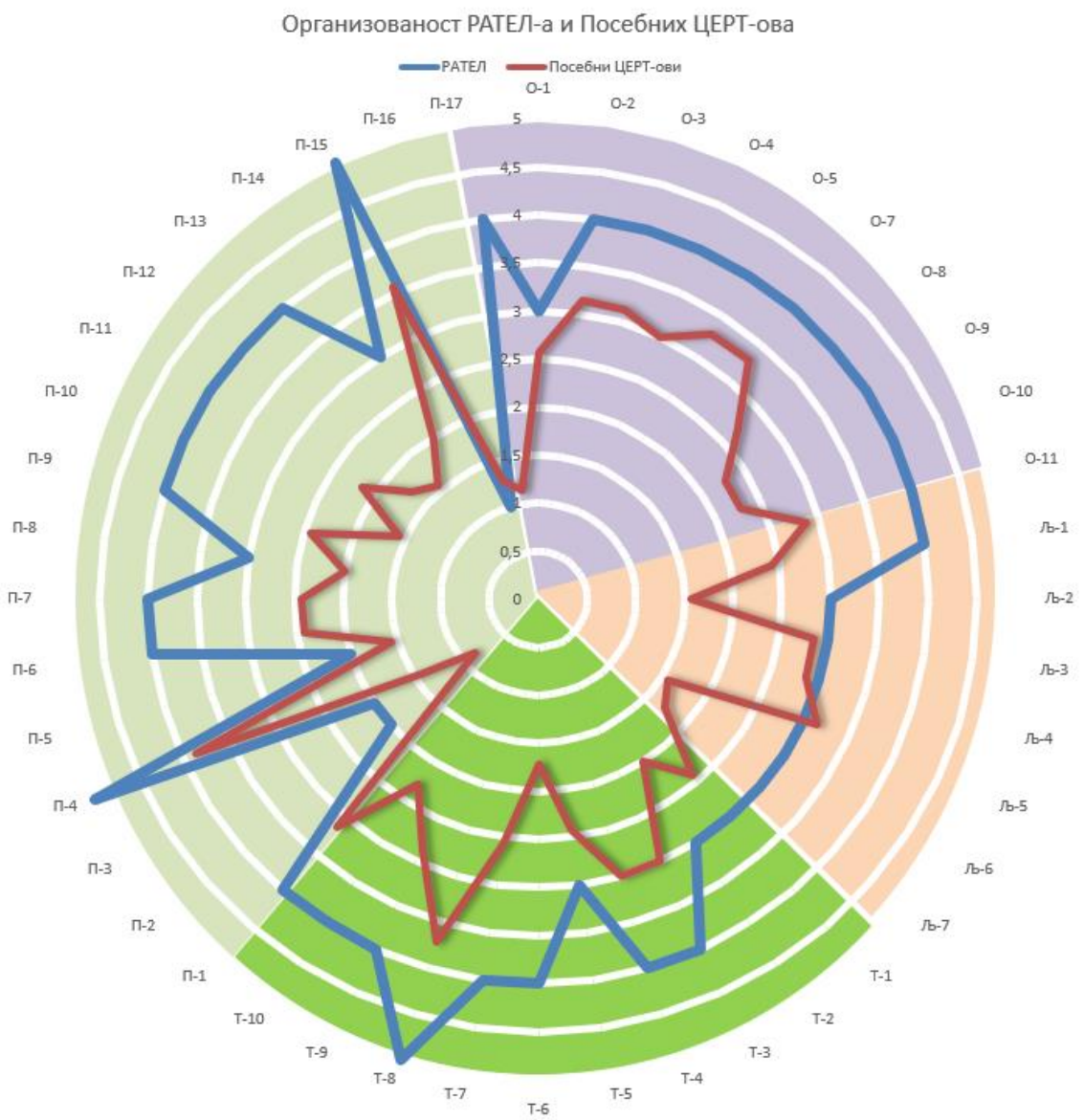
Управљање инцидентима у ИКТ системима од посебног значаја

Извор: Европска агенција за сајбер безбедност, https://www.enisa.europa.eu/

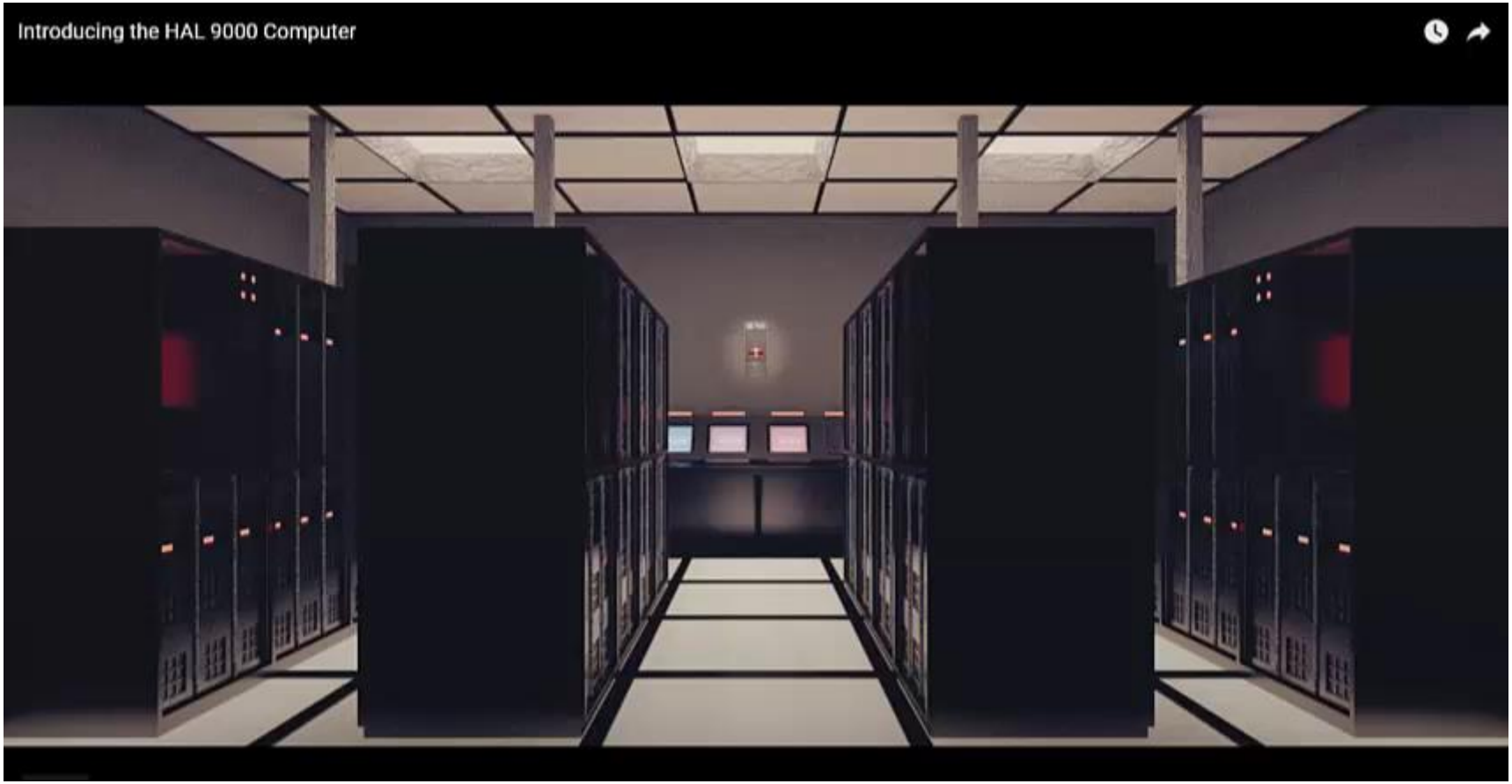
CYBERSECURITY SERBIA MAP

The Cyber Security Map of Serbia shows the most important state institutions and companies in the Republic of Serbia that are important for cyber security and incident management in information systems at the national level. The first group shows companies in the field of telecommunications (from left to right, the second group includes certification bodies that issue qualified electronic certificates, the third group includes special CERTs that are in the register of special CERTs and their superiors. The fourth group consists of banks as a special segment of security in financial transactions, the fifth group consists of large government systems and the sixth group consists of audit and consulting companies and professional organizations that provide consulting services in the field of cyber security and train people for this type of work.


ИКТ СИСТЕМИ ОД ПОСЕБНОГ ЗНАЧАЈА
ИКТ СИСТЕМИ ОД ПОСЕБНОГ ЗНАЧАЈА - ТЕЛЕКОМУНИКАЦИЈЕ
ИКТ СИСТЕМИ ОД ПОСЕБНОГ ЗНАЧАЈА – ФИНАНСИЈСКЕ ИНСТИТУЦИЈЕ
РАТЕЛ Национални ЦЕРТ
МТТТ
НАРОДНА БАНКА СРБИЈЕ
БИА (АКО ЈЕ УГРОЖЕНА НАЦ.БЕЗБЕДНОСТ)
ТУЖИЛАШТВО/ МУП ВТК (АКО ЈЕ КРИВИЧНО ДЕЛО)
ВБА (АКО ЈЕ УГРОЖЕНА ОДБРАНА ЗЕМЉЕ)


Организованост РАТЕЛ-а и Посебних ЦЕРТ-ова
РАТЕЛ
Посебни ЦЕРТ-ови
О-1
О-2
О-3
О-4
О-5
О-7
О-8
О-9
О-10
О-11
Љ-1
Љ-2
Љ-3
Љ-4
Љ-5
Љ-6
Љ-7
Т-1
Т-2
Т-3
Т-4
Т-5
Т-6
Т-7
Т-8
Т-9
Т-10
П-1
П-2
П-3
П-4
П-5
П-6
П-7
П-8
П-9
П-10
П-11
П-12
П-13
П-14
П-15
П-16
П-17
5
4,5
4
3,5
3
2,5
2
1,5
1
0,5
0

НЕДОСТАТАК АДЕКВАТНЕ РАЗМЕНЕ ИНФОРМАЦИЈА О ИНЦИДЕНТИМА СЛАБИ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ, МОЖЕ ДОВЕСТИ ДО ЕСКАЛАЦИЈЕ И ТРАЈНОГ ГУБИТКА ИНФОРМАЦИОНЕ ИМОВИНЕ

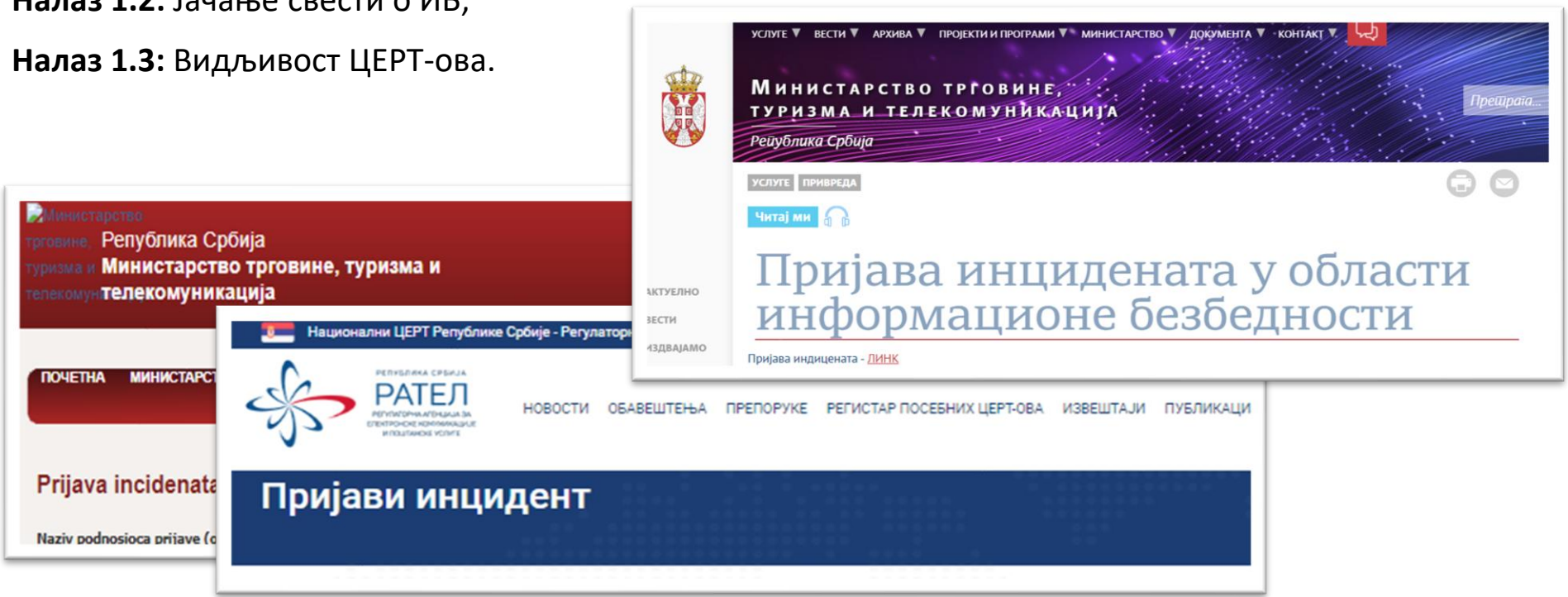


ЗАКЉУЧАК 1: Јачање сајбер отпорности и укупне информационе безбедности КИИ није могуће без утврђивања листе приоритета ИКТ СоПЗ, јачања свести о значају информационе безбедности у свим њеним аспектима и веће видљивости у јавном и интернет простору.

Налаз 1.1: Листа приоритета ИКТ СоПЗ;

Налаз 1.2: Јачање свести о ИБ;

Налаз 1.3: Видљивост ЦЕРТ-ова.



ЗАКЉУЧАК 2: Процес управљања инцидентима ИКТ СоПЗ не препознаје организациону сложеност, величину и критичност оператора за ефикасну имплементацију мера заштите, технолошка решења која користе оператори и потребу непосредног објављивања информација о инцидентима који су у току, што умањује постојеће позитивне ефекте на оснаживању сајбер отпорности.

Налаз 2.1: Категоризација оператора – обавезних мера за смањење ИТ ризика;

Налаз 2.2: Исте рањивости оператора са истим технолошким решењима;

Налаз 2.3: Алармирање јавности по пријави инцидента.

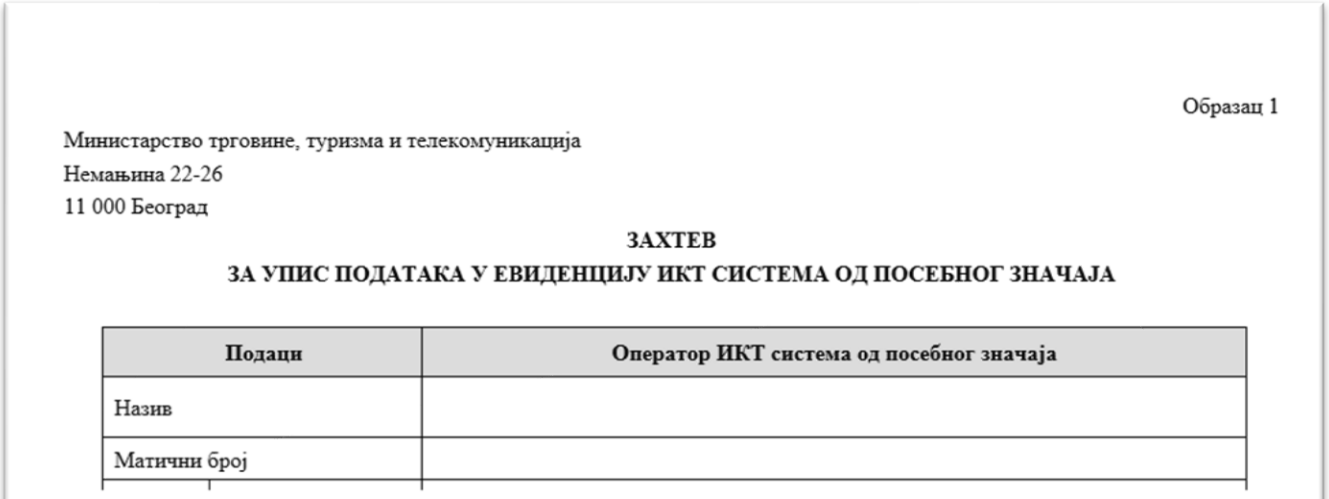
1. Управљање ризиком у вези ИКТ система;
2. Контрола приступа ИКТ систему;
3. Едукација запослених који користе ИКТ системе;
4. Безбедност података;
5. Управљање информационим добрима;
6. Чување логова активности корисника и мониторинг ИКТ система;
7. Пројектовање, изградња, одржавање и управљање ИКТ системом;
8. Управљање безбедносним инцидентима ИКТ система;
9. Управљање рањивостима и претњама током експлоатације ИКТ система;
10. Управљање услугама добављача ИКТ услуга и система;

ЗАКЉУЧАК 3: Постојећи контролни и инспекцијски механизам не обезбеђује адекватну надзорну функцију Министарства, стварајући ризик да инциденти ескалирају и угрозе информациону имовину критичне инфраструктуре.

Налаз 3.1: Евиденција оператора некомплетна;

Налаз 3.2: Евиденција без технолошких елемената;

Налаз 3.3: Недовољни инспекцијски капацитети.



Образац 1

Министарство трговине, туризма и телекомуникација
Немањина 22-26
11 000 Београд

ЗАХТЕВ
ЗА УПИС ПОДАТАКА У ЕВИДЕНЦИЈУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

Подаци	Оператор ИКТ система од посебног значаја
Назив	
Матични број	

Државна ревизорска институција дала је 9 препорука и то:

Субјект ревизије	Препоруке
1. Министарство информација и телекомуникација	1. да успоставе **листу приоритета ИКТ система** од посебног значаја према степену критичности у циљу обезбеђења ефикасног тока опоравка критичне информационе инфраструктуре. (Налаз 1.1.) – Приоритет 3 . 2. да у сарадњи са другим надлежним организацијама утврде **стварне потребе за обукама**, стручним усавршавањем, редовним обавештавањем, као и за другим активностима намењених крајњим корисницима, запосленима на ИТ пословима у државним органима и организацијама које управљају критичном информационом инфраструктуром у циљу јачања свести о значају информационе безбедности и превентивним мерама заштите. (Налаз 1.2.) – Приоритет 3. 3. да измене страницу на сајту МТТТ и преусмере кориснике на Национални CERT и апликацију за пријављивање на домену cert.rs, и пропишу ту обавезност за све CERT-ове за које су надлежни. (Налаз 1.3.) – Приоритет 3. 4. да **изврше категоризацију оператора ИКТ система** по величини и критичности, дефинишу минималне/обавезне мере према категорији оператора. (Налаз 2.1.) – Приоритет 3. 5. да у сарадњи са надлежним органима прикупе податке о технолошким решењима оператора ИКТ СоПЗ, обезбеде систем **за аутоматизовано обавештавање између CERT-ова** и партнера, обезбеде имплементацију и примену. (Налаз 2.2.) – Приоритет 3. 6. да обезбеде механизам **објављивања аларма по пријави инцидента**, означавањем врсте инцидента, нивоа опасности, анонимизоване податке о технолошким решењима погођених ИКТ СоПЗ као и могућим плановима реаговања на исте. (Налаз 2.3.) – Приоритет 3. 7. да коришћењем одговарајућих извора прибаве све неопходне податке како би могли да оцене ИТ ризике, пропишу нивое заштите по приоритетима у циљу обезбеђивања ефикасне заштите. (Налаз 3.1.) – Приоритет 3. 8. да се применом дефинисаних критеријума изврши **адекватна процена ризика за избор** надзираних субјеката.(Налаз 3.2.) –Приоритет 3. 9. да успоставе систем колегијалног прегледа од стране овлашћених лица која су компетентна за утврђивање могућих рањивости код оператора ИКТ система од посебног значаја. (Налаз 3.3.) – Приоритет 3.

Корист од ревизије:

1. Већа безбедност свих учесника у систему од потенцијалних нежељених напада и нежељеног утицаја;
2. Већа обученост учесника у систему;
3. Боља комуникација између активних учесника у систему;
4. Ефикаснији ток опоравка критичне информационе инфраструктуре;
5. Ефикасније спровођење мера заштите према категорији и значају оператора;
6. Ефикаснији механизам алармирања јавности;
7. Интезивније укључивање информатичких ресурса (ИТ стручњака и ИТ фирми) у обезбеђивању критичне информационе инфраструктуре Републике Србије.

ХВАЛА НА ПАЖЊИ!

kancelarija@dri.rs

www.dri.rs