Упитник и ревизорске процедуре за Акт о безбедности - Методолошке препоруке за израду, континуирано праћење и унапређење Акта о безбедности ИКТ система -

1. Успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система од посебног значаја (ISO 27002 контроле 6.1.1 и 6.1.2.) - Интервјуисати одговорне (ISO, ИТ сектор, ЉР, Усклађенот пословања) у вези са пословима дефинисаним овом тачком и прегледати да ли су те одговорности дефинисане интерном регулативом или у званичним описима послова тих запослених, као и да ли је та интерна регулатива и одговорности наведена у Акту о безбедности ИКТ система. Све уочене недостатке треба пописати и предложити да се одговарајућа документа ажурирају. Клијент нам може ажуриране документе доставити на разматрање. Усвајање докумената је у њиховој надлежности (Ова препорука се израду финалне верзије и усвајање генерално се односи на све мере).

   Питања:

   - Да ли је управљање информационом безбедношћу јасно препознато у организационој структури и да ли су утврђени одговарајући послови?
   - Да ли су те одговорности дефинисане интерном регулаивом или у званичним описима послова тих запослених?
   - Да ли је та интерна регулатива и одговорнсти наведена у Акту о безбедности ИКТ система?

2. **Постизање безбедности рада на даљину и употребе мобилних уређаја –** (ISO 27002 контрола 6.2.) - Прегледати сву интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведене у Акту, интервјуисати одговорне запослене, проверити да ли су те одговорности негде дефинисане, прегледати листе запослених који имају даљински приступ и који користе мобилне уређаје (*Laptop,* мобилни телефони, *iPad, smartphone, iphone...*), ако их има много, одабрати узорак, а ако не, тестирати за све, да ли је даљински приступ и употреба мобилних уређаја одобрена од стране одговорних. Додатно, прегледати техничке конфигурације система (нпр. *IBM MDM for security of iPad, smartphone, iphone,*

security of VPN connections, laptop security) које обезбеђују све дефинисано овом тачком Уредбе. (За ово је потребно мало више времена ако се ради у потпуности и детаљно).

Питања:

- Да ли је дозвољен рада са мобилних уређаја?
- Да ли је дозвољен рад на даљину?
- Да ли је дозвољен рад на даљину и са мобилних уређаја у власништву запослених или само са уређаја у власништву организације?
- Ко покреће иницијативу за дозвољавање рада на даљину и са мобилних уређаја и ко даје сагласност?
- Да ли постоје одговарајуће процедура за задуживање и раздуживање уређаја?
- Да ли су дефинисане одговорности за рад на даљину и употребу мобилних уређаја?
- Да ли су та интерна регулатива и одговорности наведене у Акту?
- Да ли постоје ажурне евиденције (листе) запослених који имају даљински приступ и који користе мобилне уређаје?
- Да ли се приликом престанка радног односа одмах враћа задужена опрема и укидају налози за удаљени приступ?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

3. **Обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност** - (ISO 27002 контрола 7.2.) - Прегледати CV-е свих одговорних запослених из тачке 1 и утврдити да ли имају одговарајуће радно искуство и образовање. Утврдити да ли постоји интерна регулатива за коришћење ИКТ система, за обуку у вези са информационом безбедношћу и покретање поступка против запослених који нарушавају информациону безбедност, као и да ли су та интерна регулатива и одговорности наведене у Акту, да ли запослени потписују да су упознати са овом регулативом, да ли постоје редовне обуке у вези информационе безбедности за све запослене и да ли се покреће поступак против запослених који нарушавају информациону безбедност. Овде се поставља и питање да ли је дефинисан дисциплински поступак, да ли постоје претходно спроведени поступци, да ли постоје записници…

Питања:

- Да ли запослени одговорни за информациону безбедност имају одговарајуће искуство и образвање (формално и неформално – додатно)?
- Да ли постоји интерна регулативе којом се уређује обука запослених?
- Да ли постоје планови редовне екстерне и интерне обуке у вези информационе безбедности?
- Да ли се утврђује буџет за екстрну и интерну обуку у области информационе безбедности?
- Да ли је претходни буџет дефонисан посебно или у оквиру укупног буџета за обуку?
- Да ли се спроводе редовне обуке у вези информационе безбедности?
- Да ли постоје евиденције о спроведеним обукама?
- Да ли се обуке понављају због запослених који из било ког разлога нису били присутгни на редовним обукама?
- Да ли се органиуују посебне обуке за новозапослене?
- Да ли постоји интерна регулативе којом се уређује одговорност запослених у области информационе безбедности (и приватности)?
- Да ли запослени потписују да су упознати регулативом којом се уређује одговорност запослених?
- Да ли се покреће поступак против запослених који нарушавају информациону безбедност?
- Да ли је дисциплински поступак дефинисан?
- Да ли су спровођени дисциплински поступци у претходном периоду?
- Да ли постоје записници о спроведеним дисциплинским поступцима?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

4. **Заштита од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система** – (ISO 27002 контрола 7.3.) - Прегледати обрасце уговора за стално и привремено запослене (по уговору или преко омладинске/студентске задруге) да ли су сви запослени обавезани уговором или другим актом да након престанка или промене радног ангажовања не откривају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система, као и да ли су ове мере наведене у Акту.

Питања:

- Да ли су сви запослени обавезани уговором или другим актом да након престанка или промене радног ангажовања не откривају поверљиве и друге информације које су од значаја за информациону безбедност ИКТ система?
- Да ли су ове мере наведене у Акту?
- Да ли се при променама послова врши ажурирање права приступа?
- Да ли је при престанку радног односа уређено раздуживање опреме и затварање свих налога за приступ информационом систему?
- Да ли о томе постоји евиденција?
- Да ли се мењају параметри за приступ групним налозима (уколико постоје) у случају да је особа којој престаје радни однос имала приступ групним налозима?

5. **Идентификовање информационих добара и одређивање одговорности за њихову заштиту –** (ISO 27002 контрола 8.1) - Проверити да ли су одговорности за ово негде дефинисане, интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, прегледати да ли постоји каталог (попис) информационих добара, путем којих се врши израда, обрада, чување, пренос, брисање и уништавање података у ИКТ систему, да ли су та добра класификована, да ли су одређене мере заштите, власници и чувари (custodian) добара, да ли се редовно (барем годишње) ради класификација.

Питања:

- Da li postoji procedura za klasifikaciju informacionih dobara?
- Da li postoji katalog (popis) informacionih dobara?
- Da li je izvršena klasifikacija informacionih dobara?
- Da li je definisano vlasnici i čuvari (*custodian*) informacionih dobara, kao i njihove odgovornosti?
- Da li se redovno (barem godišnje) radi klasifikacija?
- Da li su ta interna regulativa i odgovornosti navedene u Aktu?

6. **Класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из Закона о информационој**

безбедности - (ISO 27002 контрола 8.2) - Проверити да ли су одговорности за ово негде дефинисане, интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, проверити да ли је у склопу класификације информационих добара урађена и класификација података узимајући у обзир, важност података, штету која може да настане услед неовлашћеног откривања, измене или брисање података и прописе који уређују питања заштите података (о тајним подацима, пословној тајни, подацима о личности), проверити да ли постоје и, ако постоје, прегледати процедуре за поступање, обраду, складиштење и преношење података у складу са класификацијом података, проверити да ли су дефинисане мере заштите података, као и да ли су те мере у складу са проценом ризика.

Питања:

- Да ли је извршена класификација информационих добара?
- Да ли је у склопу класификације информационих добара урађена и класификација података узимајући у обзир, важност података, штету која може да настане услед неовлашћеног откривања, измене или брисање података и прописе који уређују питања заштите података (о тајним подацима, пословној тајни, подацима о личности)?
- Да ли постоје (и, ако постоје, прегледати) процедуре за поступање, обраду, складиштење и преношење података у складу са класификацијом података?
- Да ли су дефинисане мере заштите података, као и да ли су те мере у складу са проценом ризика?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

7. **Заштита носача података** - (ISO 27002 контрола 8.3) - Проверити да ли су одговорности за ово негде дефинисане, интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведене у Акту, проверити да ли су дефинисане и да ли се примењују процедуре за управљање носачима података у складу са класификацијом из претходног члана, да ли те процедуре укључују поступак одобравања изношења носача података из просторија оператора ИКТ система, чување носача података на безбедном месту, коришћење криптографских техника за

заштиту података када је то предвиђено прописима или када је таква врста заштите потребна, обезбеђивање сигурног преноса података на нови носач података, чување резервних копија на одвојеним носачима података, заштита носача података приликом транспорта обезбеђивањем поузданог транспорта и поузданих особа које преносе носаче података и обезбеђивањем адекватне амбалаже у циљу физичке заштите приликом транспорта, процедуре за безбедно расходовање и уништавање носача података када више нису потребни, као и да ли се у складу са шемом класификације података, води евиденција о коришћењу носача података и предузетим поступцима у вези са заштитом података и носача података.

Питања:

- Да ли су одговорности за заштиту носача података негде дефинисане?
- Да ли се примењују процедуре за управљање носачима података у складу са класификацијом из претходног члана?
- Да ли те процедуре укључују:
    - Поступак одобравања изношења носача података из просторија оператора ИКТ система?
    - Чување носача података на безбедном месту?
    - Коришћење криптографских техника за заштиту података када је то предвиђено прописима или када је таква врста заштите потребна?
    - Обезбеђивање сигурног преноса података на нови носач података?
    - Чување резервних копија на одвојеним носачима података?
    - Заштиту носача података приликом транспорта обезбеђивањем поузданог транспорта и поузданих особа које преносе носаче података и обезбеђивањем адекватне амбалаже у циљу физичке заштите приликом транспорта?
    - Безбедно расходовање и уништавање носача података када више нису потребни?
- Да ли се у складу са шемом класификације података, води евиденција о коришћењу носача података и предузетим поступцима у вези са заштитом података и носача података?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

8. **Ограничење приступа подацима и средствима за обраду података -** (ISO 27002 контрола 9.1) - Проверити да ли су одговорности за ово негде дефинисане, интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли је та интерна регулатива и одговорности наведена у Акту, проверити да ли су дефинисане и да ли се примењују политке и процедуре за логичку контролу приступа подацима и физичку контролу приступа средствима за обраду података, да ли су права приступа додељена по принципу минимално потребних и у складу са радним местом, тестирати да ли је имплементриан Identity management system који обезбеђује да сви запослени који раде на истом радном месту имају иста права – исте роле, тестирати процес одобрења, креирања и ажуирања корсиничких рола – одабрати узорак или тестирати све креиране и измењене роле у току године, да ли власници података одобравају права приступа подацима у складу са класификацијом података, да ли су имплементиране процедуре за контролу и ограничен приступ, укључујући даљински пиртсуп, мрежи и мрежним уређајима.

   Питања:

   - Да ли су одговорности за ограничење приступа подацима и средствима за обраду података негде дефинисане?
   - Да ли се примењују политике и процедуре за логичку контролу приступа подацима?
   - Да ли се примењују политике и процедуре за физичку контролу приступа подацима?
   - Да ли су права приступа додељена по принципу минимално потребних и у складу са радним местом?
   - Да ли је имплементриан Identity management system?
   - Да сви запослени који раде на истом радном месту имају иста права – исте роле?
   - Да ли власници података одобравају права приступа подацима у складу са класификацијом података?
   - Да ли су имплементиране процедуре за контролу и ограничен приступ, укључујући даљински приступ, мрежи и мрежним уређајима?
   - Да ли су та интерна регулатива и одговорности наведене у Акту?

9. **Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа -** (ISO 27002 контрола 9.2, осим 9.2.4)

- Проверити да ли су одговорности за ово негде дефинисане, интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, проверити да ли су дефинисане и да ли се примењују процедуре за одобравање и укидање корисничких права, као и промену права у случају промене радног места, тражити од ЉР листе свих новозапослених, свих запослених који су напустили фирму и променили радно место у току године, одабрати по око 10% за сваку од ових листа и тестирати да ли је за сваког запосленог из узорка креиран корснички захтев за доделу, измену и укидање корисничких права, да ли је тај захтев одобрен у складу са дефинсаним процедурама и да су права додељена/измењена/укинута у складу са захтевима, најбоље би било да је Identity management system повезан са ЉР базом и да ЉР база аутоматски шаље информацију Identity management system-у кад дође до промене статуса сваког запосленог и да то тригерује доделу, измену и укидање корисничких права; Проверити да ли сви запослени из узорка имају униqуе ИД, да ли се користе заједнички/генерички ИД, проверити да ли су администраторска права на свим ниовима (мрежа, ОС, апликације) сведена на минимално потребна, тестирати да ли се редовно (бар годишње) ради ревиеw корисницких профила (рола, права).

Питања:

- Да ли су да ли су одговорности за одобравање овлашћеног приступа и спречавање неовлашћеног приступа негде дефинисане?
- Да ли су дефинисане и да ли се примењују процедуре за одобравање и укидање корисничких права, као и промену права у случају промене радног места?
- Да ли је за сваког запосленог постоји корснички захтев за доделу, измену и укидање корисничких права?
- Да ли се ти захтеви одобрени у складу са дефинсаним процедурама и да ли су права додељена/измењена/укинута у складу са захтевима?
- Да ли постоји Identity management system повезан са ЉР базом?
- Да ли да ЉР база аутоматски шаље информацију Identity management system-у кад дође до промене статуса сваког запосленог и да то тригерује доделу, измену и укидање корисничких права?
- Да ли сви запослени имају униqуе ИД?
- Да ли се користе заједнички/генерички ИД?

- Како је уређено додељивање и администрирање налога за привремено ангажоване?
- Да ли су администраторска права на свим ниовима (мрежа, ОС, апликације) сведена на минимално потребна?
- Да ли се редовно (бар годишње) ради ревиew корисницких профила (рола, права)?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

10. **Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију** - (ISO 27002 контрола 9.2.4 i 9.3) - Прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, проверити да ли се за притсуп подацима користи username/password и двофакторска аутентикација (за high risk податке или апликације), да ли су сви запослени неким документом обавезани да не откривају те аутентикационе податке, тестирати на нивоу ОС и апликација да ли су имплементиране политике корисничких налога и лозинки, тестирати да ли се аутентикациони подаци чувају и да ли су заштићени у информационом систему на одговарајући начин.

    Питања:
    - Да ли постоје политике/процедуре/упутства корисничких налога и лозинки?
    - Да ли се аутентикациони подаци чувају и да ли су заштићени у информационом систему на одговарајући начин?
    - Да ли се за притсуп подацима користи обавезно username/password?
    - Да ли се (за хигх риск податке или апликације) користи двофакторска аутентикација?
    - Да ли су сви запослени неким документом обавезани да не откривају аутентикационе податке?
    - Да ли су та интерна регулатива и одговорности наведене у Акту?

11. **Предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података** - (ISO 27002 контрола 10) - Проверити да ли су одговорности за ово негде дефинисане, интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведена у Акту, проверити да ли су дефинисане процедуре криптозаштите, ако се криптозаштита користи тестирати да ли се користе

инсецуре протоколи/алгоритми као што су SSL, TLS 1.0, 3DES, MD5, SHA. Проверити да ли су дефинисане процедуре за управљање криптографским кључевима које укључују генерисање, складиштење, архивирање, преузимање, расподелу, повлачење и уништавање кључева.

Питања:

- Да ли је дефинисана употреба криптозаштите?
- Да ли су дефинисане одговорности у оквиру криптозаштите?
- Који криптографски протоколи се користе?
- Да ли су дефинисане процедуре за управљање криптографским кључевима које укључују генерисање, складиштење, архивирање, преузимање, расподелу, повлачење и уништавање кључева?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

12. **Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему** - (ISO 27002 контрола 11.1.2) – Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли је та интерна регулатива и одговорности наведена у Акту, проверити да ли су дефинисане процедуре физичке заштите просторија у којима се налази ИКТ систем, да ли постоје аларми, камере, да ли се користи двофакторска аутентикација за улаз у те просторије (нпр. Access card and secret PIN), да ли се захтева ношење видљивог идентификационог обележја у тим просторијама и да ли се то поштује, да ли је дефинисана листа запослених који могу да уђу у сервер собу, тражити лог у последњих нпр. годину дана и тестирати да ли су само овлашћене особе улазиле у те просторије, да ли су дебели зидови, заштићени прозори…

Питања:

- Да ли су дефинисане процедуре физичке заштите просторија у којима се налази ИКТ систем?
- Да ли се користи двофакторска аутентикација за улаз у те просторије?
- Да ли се захтева ношење видљивог идентификационог обележја у тим просторијама и да ли се то поштује?
- Да ли је дефинисана листа запослених који могу да уђу у сервер собу?

- Да ли су дебели зидови, заштићени прозори (ако их има)…?
- Да ли има цеви за воду и грејање који пролазе кроз просторију?
- Да ли постоји противпожарна опрема?
- Да ли постоји мануелна евиденција улазака у собу?
- Да ли су расположиви логови на основу којих се може утврдити ко је улазио у просторију?
- Колико дуго се чувају видео снимци?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

13. **Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем** - (ISO 27002 контрола 11.2.1) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведена у Акту, проверити да ли су дефинисане процедуре енвиронментал заштите просторија у којима се налази ИКТ систем, да ли су уграђени одговарајући противпожарни уређаји, подигнут под за заштиту од поплава, аларми/детектори за дим и воду, redundant air condition system, automatic temperature control instrument, redundant power lines that feed the server room to reduce the risk of power failure, wiring is placed in the fire-resistant panels and conduit, да ли има UPS и (дизел) агрегат у случају нестанка електричног напајања.

Питања:

- Да ли су дефинисане процедуре енвиронментал заштите просторија у којима се налази ИКТ систем?
- Да ли су уграђени одговарајући противпожарни уређаји?
- Да ли је подигнут под за заштиту од поплава?
- Да ли постоје аларми/детектори за дим и воду?
- Да ли постоји *редундантни систем климатизације*?
- Да ли постоје *инструменти за аутоматску контролу температуре*?
- Да ли постоје *редундантне електричне линије које напајају серверску собу да би се смањио ризик од нестанка струје*?
- Да ли *се ожичење поставља у ватроотпорне панеле и водове*?
- Да ли има УПС и power генератор у случају нестанка електричног напајања?
- Да ли је у претходном периоду било крађе опреме?

- Да ли су та интерна регулатива и одговорности наведене у Акту?

14. **Обезбеђивање исправног и безбедног функционисања средстава за обраду података** - (ISO 27002 контрола 12.1) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, проверити да ли су дефинисане опертивне процедуре и одговорности за руковање средствима, које се односе на отпочињање и завршетак приступа информационом систему, захтеве за планирање укључујући међузависности са другим системима, најранији почетак посла и последње време завршетка посла; руковање грешкама или другим изузетним условима, који могу настати током извршавања посла; контакти за подршку и ескалацију у случају неочекиваних оперативних потешкоћа; процедуре поновног покретања и опоравка система за употребу у случају квара система; процедуре праћења, као и процедуре за одржавање опреме, руковање носачима података; change management процедуре и одговорности. Тражити лог свих измена имплементираних у продукционо окружење у последњих годину дана, одабрати узорак (око 10% свих) и на узорку тетсирати да ли су сви захтеви за изменом анализирани и одобрени од стране одговорних особа, да ли су измене тестиране и ауторизоване за имплементацију у продукцији од стране оних који су захтевали измену, да ли постоји сегрегација дужности између развоја и операција, као и fall-back процедуре у случају потребе враћања на претходно стање пре имплементације измене, проверити да ли су међусобно одвојени развојно, тестно и продукционо (оперативно) окружење, проверити да ли су имплементиране capacity management и план.

Питања:

- Да ли су дефинисане оперативне процедуре и одговорности за руковање средствима, које се односе на отпочињање и завршетак приступа информационом систему?
- Да ли постоје процедуре/упутства за одржавање опреме?
- Да ли постоје процедуре/упутства за руковање носачима података?
- Да ли постоје change management процедуре?
- Да ли постоји сегрегација дужности између развоја и операција?
- Да ли постоје fall-back процедуре у случају потребе враћања на претходно стање пре имплементације измене?

- Да ли су међусобно одвојени развојно, тестно и продукционо (оперативно) окружење?
- Да ли су имплементиране capacity management процедуре и план?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

15. **Заштита података и средства за обраду података од злонамерног софтвера** - (ISO 27002 контрола 12.2) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, проверити да ли су дефинисане и имплементиране процедуре за заштиту од злонамерног софтвера, да ли те процедуре укључују следеће: *Политика забрањује употребу неовлашћеног софтвера; Имплементиране су контроле превенције или детекције за коришћење неовлашћеног софтвера (беле листе апликација) – проверити да ли је конфигурисано; Контроле превенције или откривања за коришћење познатих или сумњивих злонамерних веб локација су имплементиране (црна листа) - проверити да ли је конфигурисано; Прилози и преузимања е-поште се скенирају на малвер пре уласка у интерну мрежу – проверити да ли је конфигурисано; Датотеке примљене преко мрежа или преко било ког облика медија за складиштење и веб странице се скенирају у потрази за малвером – проверити да ли је конфигурисано; Редовно се прикупљају информације као што су претплата на мејлинг листе или провера веб локација које дају информације о новом малверу; Испитајте антивирусне конфигурације и узорке системских компоненти укључујући, између осталог, јавно доступне сервере и контролере домена да бисте потврдили да: Антивирусни софтвер је централно дистрибуиран и да су дефиниције актуелне; Врше се периодична скенирања рачунара; Дневници ревизије се генеришу и чувају унапред дефинисани временски период; Антивирусни софтвер активно ради и корисник не може да га онемогући или промени; Софтвер је конфигурисан да шаље обавештења одговорном особљу када се пронађу безбедносни ризици.*

Питања:

- Да ли су дефинисане и имплементиране процедуре за заштиту од злонамерног софтвера?
- Да ли те процедуре укључују следеће:
    - *Политика забрањује употребу неовлашћеног софтвера?*

- *Имплементиране су контроле за превенцију или откривање коришћења неовлашћеног софтвера (на белу листу апликација)?*
- *Да ли су имплементиране контроле превенције или откривања за коришћење познатих или сумњивих злонамерних веб локација (црна листа)?*
- *Да ли се прилози и преузимања е-поште скенирају у потрази за малвером пре уласка у интерну мрежу?*

- Да ли се антивирус софтвер централно дистрибуира?
- Да ли су дефиније ажурне?
- Да ли се спроводе перодична скенирања свих рачунара?
- Да ли антивирус софтвер стално ради?
- Да ли антивирус софтвер може бити привремено/трајно заустављен или мењани параметри од стране крајњих корисника?
- Да ли је антивирус софтвер тако конфигурисан да шаље нотификацуије одговорним особама?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

16. **Заштита од губитка података -** (ISO 27002 контрола 12.3) **-** Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, проверити да ли су дефинисане и имплементиране процедуре за заштиту од губитка података (*процедуре за прављење резервних копија) и да ли те процедуре укључују следеће: креирање, складиштење, период задржавања и обнављање података и софтвера који подржавају критичне пословне процесе; утврди да ли је најмање једна ажурирана и потпуна резервна копија ускладиштена на одговарајућој удаљености од примарног центра података узимајући у обзир потребу да се избегне утицај истих ризика на обе локације и да ли је адекватно заштићена; утврдити да ли је обнављање ове резервне копије тестирано тако да се подаци и софтвер који подржавају критичне пословне процесе могу вратити како би се омогућило поновно успостављање пословних процеса у оквиру циљаног времена опоравка; утврдити да ли су документоване процедуре које се односе на опоравак података изгубљених између последње резервне копије и времена катастрофе.*

Питања:

- Да ли су дефинисане и имплементиране процедуре за заштиту од губитка података (бацкуп процедуре)?
- Да ли те процедуре укључују следеће:
    - *Креирање, складиштење, период задржавања и обнављање података и софтвера који подржавају критичне пословне процесе?*
    - *Утврдите да ли се најмање једна ажурирана и потпуна резервна копија чува на одговарајућој удаљености од примарног центра података, узимајући у обзир потребу да се избегне утицај истих ризика на обе локације и да ли је адекватно заштићена?*
    - *Утврдите да ли је обнављање ове резервне копије тестирано тако да се подаци и софтвер који подржавају критичне пословне процесе могу вратити како би се омогућило поновно успостављање пословних процеса у оквиру циљаног времена опоравка?*
    - *Утврдите да ли су процедуре за опоравак података изгубљених између последње резервне копије и времена катастрофе документоване*?

Да ли су та интерна регулатива и одговорности наведене у Акту?

17. **Чување података о догађајима који могу бити од значаја за безбедност ИКТ система** - (ISO 27002 контрола 12.4) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведена у Акту, проверити да ли су дефинисане и имплементиране процедуре за чување података о догађајима у вези активности корисника, грешкама и догађајима у вези са информационом безбедношћу, а који се морају чувати и редовно проверавати (log management). Увидом у конфигурацију лог манагемент алата проверити следеће: *Кршења прага (events) пријављена од стране алата за надзор безбедности инфраструктуре, активности корисника, администратора система и оператера система се евидентирају у алатима за управљање безбедносним инцидентима и догађајима; Објекти за евидентирање и информације из дневника су заштићени од неовлашћеног приступа; Сатови свих релевантних система за обраду информација су синхронизовани на један референтни извор времена; Редовно праћење, преглед и анализа евиденције догађаја се спроводи за потенцијалне инциденте; Карте за инциденте се креирају благовремено када праћење идентификује потенцијалне безбедносне инциденте; Период чувања лог фајлова је дефинисан да би се помогло у будућим истрагама*.

Питања:

- Да ли је *log management*алат конфигурисан тако да су:
    - *Кршења прага (events) пријављена од стране алата за надзор безбедности инфраструктуре, активности корисника, администратора система и оператера система се евидентирају у алатима за управљање безбедносним инцидентима и догађајима?*
    - *Објекти за евидентирање и подаци из дневника су заштићени од неовлашћеног приступа?*
    - *Сатови свих релевантних система за обраду информација су синхронизовани са једним референтним извором времена?*
    - *Да ли се редовно надгледа, прегледа и анализира евиденција догађаја за потенцијалне инциденте?*
    - *Карте за инциденте се праве благовремено када се праћењем идентификују потенцијални безбедносни инциденти?*
    - *Период задржавања лог фајлова је дефинисан да би се помогло у будућим истрагама*?
- Да ли је претходно наведено у политици информационе безбедности и дефинисано у неким процедурама/упутствима и да ли су та интерна регулатива и одговорности наведене у Акту?

18. **Обезбеђивање интегритета софтвера и оперативних система** - (ISO 27002 контрола 12.5) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли је та интерна регулатива и одговорности наведена у Акту, проверити да ли су дефинисане и имплементиране процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, ажурирање софтвера и оперативних система од стране овлашћеног администратора (тестирати ко има приступ оперативним системима и да ли постоји интерна регулатива за инсталацију софтвера), примена система за контролу конфигурације софтвера (да ли се користи), успостављање могућности повратка на претходно стање пре имплементације промена у систему, чување претходних верзија софтвера у случају неочекиваних ситуација, као и *audit log of all updates to operational program libraries*.

Питања:

- Да ли су дефинисане и имплементиране процедуре којима се обезбеђује контрола интегритета инсталираног софтвера и оперативних система, ажурирање софтвера и оперативних система од стране овлашћеног администратор?
- Ко све има приступ оперативним системима и да ли постоји интерна регулатива за инсталацију софтвера), примена система за контролу конфигурације софтвера?
- Да ли је уређено успостављање могућности повратка на претходно стање пре имплементације промена у систему, чување претходних верзија софтвера у случају неочекиваних ситуација, као и audit log of all updates to operational program libraries?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

19.Заштита од злоупотребе безбедносних слабости ИКТ система - (ISO 27002 контрола 12.6) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведене у Акту, проверити да ли су дефинисане и имплементиране *patch management* procedure, тестирати да ли *процес управљања закрпама обезбеђује да су све актуелне, релевантне закрпе, сервисни пакети и друга ажурирања софтвера и оперативног система примењене након документованог тестирања закрпа и одобрења од стране овлашћених страна (сва критична безбедносна ажурирања треба да се имплементирају у року од 1 месеца, а сва друга безбедносна ажурирања треба да се примени у року од 2-3 месеца од објављивања),* проверити да ли су дефинисане процедуре за Penetration tests и vulnerability assessments, увидом у одговарајуће извештаје проверити да ли се Penetration tests и vulnerability assessments раде редовно; да ли су поред екстерних тестирају и интерне адресе, да ли се извештаји комуницирају техничком особљу и менаџменту, као и да ли се идентификоване слабости отклањају.

Питања:

- Да ли су дефинисане и имплементиране патцх манагемент процедуре?
- Да ли *patch management process* obezbeđuje da *све актуелне, релевантне закрпе, сервисни пакети и друга ажурирања софтвера и оперативног система јесу примењена након документованог тестирања закрпа и одобрења од стране*

овлашћених страна (сва критична безбедносна ажурирања треба да се имплементирају у року од 1 месеца, а сва остала безбедносна ажурирања треба да буду имплементирана у року од 2 -3 месеца од изласка)?

- Да ли су дефинисане процедуре за *penetration* тестове и *vulnerability assessments*?
- Да ли постоје одговарајући penetration тестове и vulnerability assessments извештаји и како се чувају?
- Да ли се penetration тестови и vulnerability assessments раде редовно?
- Да ли су поред екстерних тестирају и интерне адресе?
- Да ли се извештаји комуницирају техничком особљу и менаџменту?
- Да ли се идентификоване слабости отклањају?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

20. **Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система –** Потребно је планирати ревизију ИКТ система са релевантним представницима ИТ-а и пословних функција како би се остварио што мањи утицај на редовно функционисање система. Уколико се током ревизије оствари већи утицај на функционисање система потребно је одговарајуће поступке прекинути или одложити.

    Питања:

    - Да ли се ревизијаИКТ система планира са релевантним представницима ИТ-а?
    - Ко спроводи интерну ИТ ревизију?
    - Да ли се спроводи ексерна ИТ ревизија?
    - Да ли су расположиви извештаји ИТ ревизија?
    - Да ли су дефинисани рокови за уклањање неусклађености и које задужен за то?
    - Да ли је менаџмент упзнат са извештајима ИТ ревизија и да ли прати спровођење отклањања примедби?
    - Да ли су та интерна регулатива и одговорности наведене у Акту?

21. **Заштита података у комуникационим мрежама укључујући уређаје и водове -** (ISO 27002 контрола 13.1) **-** Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, проверити да ли су дефинисане и имплементиране network security манагемент процедуре, као да ли је имплементирано следеће: *врсте*

контрола, као што су демилитаризоване зоне (DMZ), сегментација мреже, прокси услуге, сигуран даљински приступ; заштитни зидови на свакој интернет вези и између било које DMZ и зоне интерне мреже; сви непотребни подразумевани налози су уклоњени или онемогућени пре него што се мрежна компонента инсталира, а подразумеване лозинке укључујући SNMP низове су промењене у „јаке“ у свим заштитним зидовима, рутерима, кључним прекидачима и WiFi контролерима; преглед скупова правила заштитног зида и рутера се спроводи најмање сваких шест месеци; формални процес управљања променама за промене конфигурација рутера и заштитног зида; Мрежни дијаграм је ажуран, укључује све конекције на мрежу и конзистентан је са конфигурацијама заштитних зидова и рутера; Интерна мрежа је сегментирана и интерна мрежа је на свом сегменту мреже; DMZ је имплементиран да ограничи улазни саобраћај на Интернет само на ИП адресе и овлашћене јавно доступне сервисе (имејл, веб). Нешифровани (небезбедни) протоколи као што су SSL, HTTP, Telnet, FTP, TFTP, SNMP v1 и v2, SSH нису коришћени у заштитним зидовима, рутерима, кључним прекидачима и WiFi контролерима или је документовано пословно оправдање за њихову употребу; Сав административни приступ без конзоле заштитним зидовима, рутерима, прекидачима језгра и WiFi контролеру је шифрован коришћењем јаке криптографије; Заштитни зидови спречавају откривање приватних ИП адреса и рутирање информација са интерних мрежа на Интернет, на пример коришћењем NAT -а; Принцип подразумеваног одбијања по коме се одбија сав саобраћај осим оног који је изричито захтеван је имплементиран у правила заштитног зида; Стање или динамичко филтрирање (само „успостављене“ везе су дозвољене у мрежи) се имплементира у заштитним зидовима; Спроводе се мере против лажирања, на пример блокирање саобраћаја који потиче са Интернета са интерном изворном адресом; Само поуздане мреже и клијенти имају VPN приступ; VPN везе су обезбеђене употребом јаке криптографије; VPN везе су ограничене на неопходне сервере и услуге; Подељено тунелирање је онемогућено да би се спречило да потенцијални нападачи на дељеној мрежи компромитују удаљени рачунар и користе га за приступ интерној мрежи. Бежично умрежавање је обезбеђено употребом јаке криптографије са WiFi заштићеним приступом (WPA2); Све фабричке поставке при инсталацији укључујући, али не ограничавајући се на ИД-ове корисника администратора, лозинке/фразе на приступним тачкама, WPA кључ, Service Set Identifier (SSID) и подразумеване низове SNMP заједнице, промењене су у „јаке“

приступне фразе; Заштитни зидови периметра се инсталирају између свих бежичних мрежа и интерне мреже и дозвољавају само ауторизовани саобраћај са бежичне мреже која користи безбедност Интернет протокола (IPSec). **Ово захтева пуно времена за тестирање ако се у потпуности ради – то може бити посао за себе.**

Питања:

- Да ли су дефинисане и имплементиране network сецуриту манагемент процедуре?
- Да ли је имплементирано следеће:
    - *Types of controls, such as demilitarized zones* (DMZs)?
    - *Network segmentation?*
    - *Proxy services?*
    - *Secure remote access?*
    - *Firewalls at each Internet connection and between any DMZ and the internal network zone?*
    - *All unnecessary default accounts are removed or disabled before a network component is installed and default passwords including SNMP strings have been changed to "strong" in all firewalls, routers, core switches and WiFi controller?*
    - *A review of firewall and router rule sets is conducted at least every six months?*
    - *Fformal change management process for changes to the router and firewall configurations?*
    - *Network diagram is up-to-date, it includes all connections to the network and it is consistent with configurations of firewalls and routers?*
    - *The internal network is segmented and the internal network is on its own network segment?*
    - *DMZ is implemented to limit Internet inbound traffic to only the IP addresses and authorized publicly accessible services (e-mail, web)?*
    - *Unencrypted (insecure) protocols like SSL, HTTP, Telnet, FTP, TFTP, SNMP v1 and v2, SSH have not been used in firewalls, routers, core switches and WiFi controller or business justification for their use is documented; All non-console administrative access to firewalls, routers, core switches and WiFi controller has been encrypted by using strong cryptography?*

- *Firewalls prevent the disclosure of private IP addresses and routing information from internal networks to the Internet, for example by using the NAT?*
- *Default-deny principle by which all traffic is denied except that which is explicitly required has been implemented into firewalls' rules?*
- *Stateful or dynamic filtering (only "established" connections are allowed into the network) is being implemented in the firewalls?*
- *Anti-spoofing measures are implemented, for example block traffic originating from the Internet with an internal source address?*
- *Only trusted networks and clients have VPN access?*
- *VPN connections are secured by using strong cryptography?*
- *VPN connections are limited to necessary servers and services?*
- *Split tunneling is disabled to prevent potential attackers on the shared network to compromise the remote computer and use it to gain access to the internal network.*
- *Wireless networking has been secured by using strong cryptography with WiFi Protected Access (WPA2)?*
- *All factory defaults at installation including, but not limited to the administrator user IDs, passwords/phrases on access points, WPA key, Service Set Identifier (SSID) and default SNMP community strings have been changed to "strong" passphrases?*
- *Perimeter firewalls are installed between all wireless networks and the internal network permitting only authorized traffic from a wireless network that uses Internet protocol security (IPSec)?*

- Да ли су та интерна регулатива и одговорности наведене у Акту?

22. **Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система** - (ISO 27002 контрола 13.2) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, проверити да ли је интерном регулативом регулисана размена података са трећим лицима, да ли су са свим трећим лицима са којима се размењују подаци путем комуникационих мрежа потписани споразуми о преносу података и споразуми о поверљивости или неоткривању који садрже одредбе о безбедности преноса података.

Питања:

- Да ли је интерном регулативом регулисана размена података са трећим лицима?
- Да ли су са свим трећим лицима са којима се размењују подаци путем комуникационих мрежа потписани споразуми о преносу података и споразуми о поверљивости или неоткривању који садрже одредбе о безбедности преноса података?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

23.Питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система - (ISO 27002 контрола 14.1) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, прегледати пројектну документацију за интерни и екстерни развој пословних апликација, као и захтеве за набавком пословних апликација и утврдити да ли су у исту укључени information security захтеви, као што су захтеви за контролом права приступа подацима, transaction logging and monitoring, интерфејси са другим апликацијама. Утврдити и да ли су ови захтеви тетсирани у тест окружењу пре имплементације у продукцију, као и да ли су укључени у уговоре са трећим странама, у случају екстерног развоја. За интернет апликације треба укључити додатне контроле као што су: двофакторска аутентикација, захтеви за поверљивост и интегритет података, непорецивост транскација, енкрипција, PKI, digital signatures.

Питања:

- Да ли је уређен интерни и екстерни развој пословних апликација?
- Да ли у су у захтеве за набавком пословних апликација укључени информатион сецуриту захтеви, као што су захтеви за контролом права приступа подацима, transaction logging and monitoring, интерфејси са другим апликацијама?
- Да ли су ови захтеви тетсирани у тест окружењу пре имплементације у продукцију?
- Да ли су укључени у уговоре са трећим странама, у случају екстерног развоја.
- Да ли су за интернет апликације укључиене додатне контроле као што су: двофакторска аутентикација, захтеви за поверљивост и интегритет података, непорецивост транскација, енкрипција, PKI, digital signatures?

- Да ли су та интерна регулатива и одговорности наведене у Акту?

24. **Заштита података који се користе за потребе тестирања ИКТ система односно делова система** - (ISO 27002 контрола 14.3) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, тестирати да ли су приступна права подацима у тестним окружењима иста као и у продукцији, да ли постоје посебне ауторизације за копирање продукционог окружења у тестно, да ли се подаци бришу из тестног окружења одмах после тестрирања, да ли се копирање продукционог окружења у тестно и приступ тестним подацима уписује у *log file*.

Питања:

- Да ли су приступна права подацима у тестним окружењима иста као и у продукцији?
- Да ли постоје посебне ауторизације за копирање продукционог окружења у тестно?
- Да ли се подаци бришу из тестног окружења одмах после тестрирања?
- Да ли се копирање продукционог окружења у тестно и приступ тестним подацима уписује у log file?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

25. **Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга** - (ISO 27002 контрола 15.1) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, проверити да ли је прописан ниво доступности и врста информација и средства којима могу да приступе пружаоци услуга, за сваког пружаоца услуга, начине приступа информацијама и средствима и надзор над приступом (нпр. сви пружаоци услуга који имају информацијама приступ требало би да имају приступ лимитиран само на сервере које одржавају), проверити све уговоре са пружаоцима услуга и видети да ли је потписан NDA, уговор о поверљивости, право на ревизију пружаоца услуга, као и да ли су пружаоци услуга обавезани да обављају услуге у складу са Законом о информационој безбедности, Законом о заштити личних података и осталом законском регулативом (Законом о банкама) …

Питања:

- Да ли је прописан ниво доступности и врста информација и средства којима могу да приступе пружаоци услуга?
- Да ли су дефинисани за сваког пружаоца услуга начини приступа информацијама и средствима и надзор над приступом?
- Да ли постоје уговори са свим пружаоцима услуга?
- Да ли је са свима потписан NDA (уговор о поверљивости), право на ревизију пружаоца услуга, као и да ли су пружаоци услуга обавезани да обављају услуге у складу са Законом о информационој безбедности, Законом о заштити личних података и осталом законском регулативом (Законом о банкама) …?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

26. **Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга** - (ISO 27002 контрола 15.2) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведена у Акту, проверити да ли је успостављен механизам надзора над сваким пружаоцем услуга, да ли је именовано лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности, нпр. праћењем SLA *performance* извештаја.

Питања:

- Да ли је успостављен механизам надзора над сваким пружаоцем услуга?
- Да ли је именовано лице које је задужено за праћење реализације пружања услуга и контролу испуњености нивоа информационе безбедности?
- Да ли се прате SLA *performance* извештаји?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

27. **Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама** - (ISO 27002 контрола 16) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведени у Акту, проверити да ли је постоје процедуре којима се дефинишу одговорна лица задужена за превенцију и реаговање, план

поступања у случају опасности од настанка безбедносних инцидената или настанка безбедносних инцидената, да ли се води евиденција о предузетим активностима, проверити да ли се врши извештавање и размена информација о безбедносним слабостима ИКТ система, инцидентима и претњама, све у складу са Уредбом о Поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја. Проверити да ли су сви запослени и пружаоци услуга обавезани да одговорном лицу из става 1. овог члана без одлагања пријаве безбедносне слабости, претње и инциденте у ИКТ систему; да ли је одређено одговорно лице за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности; да ли постоје процедуре које треба да обезбеде процесе за идентификацију, прикупљање и чување информација које могу да послуже као доказ ради покретања дисциплинског, прекршајног или кривичног поступка.

Питања:

- Да ли је постоје процедуре којима се дефинишу одговорна лица задужена за превенцију и реаговање, план поступања у случају опасности од настанка безбедносних инцидената или настанка безбедносних инцидената?
- Да ли се води евиденција о предузетим активностима?
- Да ли се врши извештавање и размена информација о безбедносним слабостима ИКТ система, инцидентима и претњама, све у складу са Уредбом о Поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја?
- Да ли су сви запослени и пружаоци услуга обавезани да одговорном лицу из става 1. овог члана без одлагања пријаве безбедносне слабости, претње и инциденте у ИКТ систему?
- Да ли је одређено одговорно лице за обавештавање надлежних органа о инцидентима у ИКТ систему који могу да имају значајан утицај на нарушавање информационе безбедности?
- Да ли постоје процедуре које треба да обезбеде процесе за идентификацију, прикупљање и чување информација које могу да послуже као доказ ради покретања дисциплинског, прекршајног или кривичног поступка?

- Да ли су та интерна регулатива и одговорности наведене у Акту?

28. Мере које обезбеђују континуитет обављања послова у ванредним околностима - (ISO 27002 контрола 17) - Интервјуисати одговорне запослене, прегледати интерну регулативу којом је ово дефинисано, као и да ли су та интерна регулатива и одговорности наведене у Акту, проверити да ли је постоје мере којима се обезбеђује обављање послова у ванредним околностима, а које подразумевају одржавање информационе безбедности на задовољавајућем нивоу, тј. да ли постоје *bussines continuity* планови и да ли они обухватају захтеве за одржавање информационе безбедности, да ли су дефинисане одговорности и поступци, начини комуникације, комуникација са вендорима у случају ванредних догађаја, да ли постоји процедура/план за опоравак ИКТ система. Да ли је урађена BIA (*Business Impact Analysys*), да ли су идентификовани сви критични процеси, да ли су идентификовани RTO и RPO тих критичних процеса; да ли постоји IT *disaster recovery* план који обухвата сву опрему која подржава критичне процесе; да ли се *Business Continuity* и IT *Disaster Recovery* планови редовно (годишње) тестирају и ажурирају у складу са резултатима теста и променама у пословним процесима.

Питања:

- Да ли је постоје мере којима се обезбеђује обављање послова у ванредним околностима?
- Да ли постоји BCP?
- Да ли обухвата захтеве за одржавање информационе безбедности?
- Да ли су дефинисане одговорности и поступци, начини комуникације, комуникација са вендорима у случају ванредних догађаја?
- Да ли постоји процедура/план за опоравак ИКТ система?
- Да ли је урађена BIA (*Business Impact Analysys*)?
- Да ли су идентификовани сви критични процеси?
- Да ли су идентификовани RTO и RPO тих критичних процеса?
- Да ли постоји IT *disaster recovery* план који обухвата сву опрему која подржава критичне процесе?
- Да ли се *Business Continuity* и IT *Disaster Recovery* планови редовно (годишње) тестирају и ажурирају у складу са резултатима теста и променама у пословним процесима?

- Да ли су та интерна регулатива и одговорности наведене у Акту?