Ревизорске процедуре и упитник за Акт о безбедности ИКТ система

Методолошке препоруке за израду, континуирано праћење, унапређење и ревизију Акта о безбедности ИКТ система

Садржај

Закон о информационој безбедности

Предмет уређивања

Члан 1.

Овим законом се уређују мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

ИКТ системи од посебног значаја

Члан 6.

ИКТ системи од посебног значаја су системи који се користе:

1) **у обављању послова у органима власти**;

2) за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности;

...

Начела

Члан 3.

Приликом планирања и примене мера заштите ИКТ система треба се руководити начелима:

1. **Начело управљања ризиком**: Избор и ниво примене мера се заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредних околности;
2. **Начело свеобухватне заштите**: Мере се примењују на свим организационим, физичким и техничко-технолошким нивоима, као и током целокупног животног циклуса ИКТ система;
3. **Начело стручности и добре праксе**: Мере се примењују у складу са стручним и научним сазнањима и искуствима у области информационе безбедности;
4. **Начело свести и оспособљености**: Сва лица која својим поступцима ефективно или потенцијално утичу на информациону безбедност треба да буду свесна ризика и поседују одговарајућа знања и вештине.

Обавезе оператора ИКТ система од посебног значаја

Члан 6а

Оператор ИКТ система од посебног значаја у складу са овим законом у обавези је да:

1) упише ИКТ систем од посебног значаја којим управља у евиденцију оператора ИКТ система од посебног значаја;

2) предузме мере заштите ИКТ система од посебног значаја;

3) донесе акт о безбедности ИКТ система;

4) врши проверу усклађености примењених мера заштите ИКТ система са актом о безбедности ИКТ система и то најмање једном годишње;

5) уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико поверава активности у вези са ИКТ системом од посебног значаја трећим лицима;

6) доставља обавештења о инцидентима који значајно угрожавају информациону безбедност ИКТ система;

7) достави тачне статистичке податке о инцидентима у ИКТ систему.

Акт о безбедности ИКТ система од посебног значаја

Члан 8.

Оператор ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система.

Актом из става 1. овог члана одређују се мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја.

Акт из става 1. овог члана мора да буде усклађен с променама у окружењу и у самом ИКТ систему.

Оператор ИКТ система од посебног значаја је дужан да самостално или уз ангажовање спољних експерата врши проверу усклађености примењених мера ИКТ система са актом из става 1. овог члана и то најмање једном годишње и да о томе сачини извештај.

Ближи садржај акта из става 1. овог члана, начин провере ИКТ система од посебног значаја и садржај извештаја о провери уређује Влада на предлог Надлежног органа.

Закон о информационој безбедности - Уредбе

- Уредба о **утврђивању Листе** послова у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја

- Уредба о ближем **садржају** акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја

- Уредбу о ближем **уређењу мера** заштите информационо-комуникационих система од посебног значаја

- Уредбу о поступку достављања података, листи, врстама и значају инцидената и **поступку обавештавања** о инцидентима у информационо-комуникационим системима од посебног значаја

Циљеви Акта о безбедности

- **Одређивање начина и процедура** за постизање и одржавање адекватног нивоа безбедности система;
- **Спречавање и ублажавање последица** инцидената којим се угрожава или нарушава информациона безбедност;
- **Подизање свести** код запослених о значају информационе безбедности, ризицима и мерама заштите приликом коришћења ИКТ система;
- **Прописивање овлашћења и одговорности** запослених у вези са безбедношћу и ресурсима ИКТ система;
- Свеукупно **унапређење информационе безбедности** и провера усклађености примене мера заштите.

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 (лице задужено за безбедност информација, 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.

Питања за 1. меру

- 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 су та интерна регулатива и одговорности наведени 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 приступ за рад на даљину 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 за 2. меру

- 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 ЦВ-е свих одговорних запослених из тачке (мере) 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 за 3. меру (1)

- 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 екстерну и интерну обуку у области информационе безбедности?
- Да ли је претходни буџет дефинисан 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?

Питања за 3. меру (2)

- Да ли се организују 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).
- Проверити 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
- Проверити да ли су ове мере наведене у Акту.

Питања за 4. меру

- 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 за 5. меру

- Да ли постоји процедура за класификацију информационих добара?
- Да ли постоји каталог (попис) информационих добара?
- Да ли је извршена класификација информационих добара?
- Да ли су дефинисано власници и чувари (*custodian*) информационих добара, као и њихове одговорности?
- Да ли се редовно (барем годишње) ради класификација?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

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 за 6. меру

- 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 за 7. меру

- 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 ажуиранаја 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 пирступ, мрежи и мрежним уређајима.

Питања за 8. меру

- 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 ли 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 (1)

- ISO 27002 контрола 9.2, осим 9.2.4
- Проверити да ли су одговорности за ово 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;

9. Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа (2)

- 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 за 9. меру (1)

- 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 кориснички 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?

Питања за 9. меру (2)

- 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 ревиеw корисницких профила (улога, права)?
- Да ли су та интерна регулатива и одговорности наведене у Акту?

10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију

- ISO 27002 контроле 9.2.4 и 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 за 10. меру

- 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 high risk 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 *insecure* 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 за 11. меру

- 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 наведени 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;
- Проверити 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 за 12. меру

- 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 за 13. меру

- 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 редундантни доводи електричне линије који напајају серверску собу да би се смањио ризик од нестанка струје ?
- Да ли се каблови/водови постављају у ватроотпорне панеле и водове?
- Да ли има UPS и агрегат 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 (1)

- 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 оперативне процедуре и одговорности за руковање средствима, које се односе на отпочињање и завршетак приступа информационом систему, укључујући *scheduling requirements including interdependencies with other systems, earliest job start and the latest job completion time; handling errors or other exceptional conditions, which might arise during job execution; support and escalation contacts in the event of unexpected operational difficulties; system restart and recovery procedures for use in the event of system failure; monitoring procedures*, као и процедуре за одржавање опреме, руковање носачима података; *change management procedure* и одговорности.

14. Обезбеђивање исправног и безбедног функционисања средстава за обраду података (2)

- Тражити запис 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 procedure 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 procedure и план.

Питања за 14. меру

- 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 procedure 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 (1)

- 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;
  - Имплементиране су контроле превенције или откривања за коришћење познатих или сумњивих злонамерних веб локација (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;

15. Заштита података и средства за обраду података од злонамерног софтвера (2)

- Датотеке примљене преко мрежа или преко било ког облика медија з а складиштење и веб страница 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 то проверили*:*
  - Антивирусни софтвер се дистрибуира централно и дефиниције су актуелне;
  - Врши се периодично скенирање 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 за 15. меру (1)

- Да ли су дефинисане и имплементиране процедуре за заштиту од злонамерног софтвера?
- Да ли те процедуре укључују следеће:
  - *Политика забрањује коришћење неовлашћеног софтвера?*
  - *Да ли су имплементиране контроле за спречавање или откривање коришћења неовлашћеног софтвера (на белој листи апликација)?*
  - *Да ли су имплементиране контроле превенције или откривања за коришћење познатих или сумњивих злонамерних веб локација (на црној листи)?*
  - *Да ли се прилози е-поште и преузимања скенирају у потрази за малвером пре уласка у интерну мрежу?*

Питања за 15. меру (2)

- 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 (1)

- 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 (backup procedure) и да ли те процедуре укључују следеће :
  - *креирање, складиштење, период задржавања и обнављање података и софтвера који подржавају критичне пословне процесе;*
  - *утврдити да ли је најмање једна ажурирана и потпуна резервна копија ускладиштена на одговарајућој удаљености од примарног дата центра, узимајући у обзир потребу да се избегне утицај истих ризика на обе локације и да ли је адекватно заштићена;*

16. Заштита од губитка података (2)

- *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 документовани поступци за решавање опоравка података изгубљених између последње резервне копије и времена катастрофе.*

Питања за 16. меру

- Да ли су дефинисане и имплементиране процедуре за заштиту од губитка података (*backup* procedure)?
- Да ли те процедуре укључују следеће :
  - *Креирање, складиштење, период задржавања и рестаурација података и софтвера који подржавају критичне пословне процесе?*
  - *Утврђивање 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?*
  - *Утврђивање 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?*
  - *Утврђивање да ли су процедуре за решавање опоравка 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 (1)

- 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*).

17. Чување података о догађајима који могу бити од значаја за безбедност ИКТ система (2)

- Увидом у конфигурацију log management алата проверити следеће :
  - *Кршења прага (догађаји) 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;*
  - *Записи о инцидентима се креирају благовремено када праћење идентификује потенцијалне безбедносне инциденте;*
  - *Период чувања лог фајлова је дефинисан да би се помогло у будућим истрагама.*

Питања за 17. меру

- Да ли је *log management*алат конфигурисан тако да:
  - *Кршења прага (догађаји) 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?*
  - *Да ли су објекти за евидентирање и информације из дневника заштићени од неовлашћеног приступа?*
  - *Да ли су сатови свих релевантних система за обраду информација синхронизовани на један референтни извор времена?*
  - *Да ли се спроводи редовно праћење, преглед и анализа дневника догађаја за потенцијалне инциденте?*
  - *Да ли се пријаве за инциденте креирају на време када праћење идентификује потенцијалне безбедносне инциденте?*
  - *Да ли је период чувања лог фајлова 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 за 18. меру

- 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 (1)

- 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 патцх манагемент процедуре.
- Тестирати да ли *patch management process* обезбеђује da све актуелне, релевантне закрпе, сервисни пакети и друге исправке софтвера и оперативног система јесу примењене након документованог тестирања закрпа и одобрења од стране овлашћених страна (сва критична безбедносна ажурирања треба да буду имплементирана у року од 1 месеца, а сва остала безбедносна ажурирања треба да се имплементирају у року од 2 -3 месеца од изласка).

19. Заштита од злоупотребе безбедносних слабости ИКТ система (2)

- Проверити да ли су дефинисане процедуре за *penetration* тестове и *vulnerability assessments*.
- Увидом у одговарајуће извештаје проверити да ли се *Penetration tests and 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.

Питања за 19. меру

- Да ли су имплементиране *patch management* процедуре?
- Да ли *patch management process* обезбеђуједа све актуелне, релевантне закрпе, сервисни пакети и друге исправке софтвера и оперативног система јесу примењене након документованог тестирања закрпа и одобрења од стране овлашћених страна (сва критична безбедносна ажурирања треба да буду имплементирана у року од 1 месеца, а сва остала безбедносна ажурирања треба да се имплементирају у року од 2 -3 месеца од изласка)?
- Да ли су дефинисане процедуре за *penetration* test и *vulnerability assessments*?
- Да ли постоје одговоарајући *penetration* test и *vulnerability assessments извештаји* и како се чувају?
- Да ли се *Penetration tests u 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 за 20. меру

- Да ли се ревизија ИКТ 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?

21. Заштита података у комуникационим мрежама укључујући уређаје и водове (1)

- 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 сецуриту манагемент процедуре, као да ли је имплементирано следеће:
  - врсте контрола, као што су демилитаризоване зоне (ДМЗ), сегментација мреже, прокси услуге, сигуран даљински приступ;
  - заштитни зидови на свакој интернет вези и између било које ДМЗ 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 контролеру;
  - преглед сетова правила заштитног зида и рутера се спроводи најмање сваких шест месеци;
  - формални процес управљања променама за промене конфигурација рутера и заштитног зида;

21. Заштита података у комуникационим мрежама укључујући уређаје и водове (2)

- *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;*
- *ДМЗ је имплементиран да ограничи долазни интернет саобраћај само на ИП адресе и овлашћене јавно доступне сервисе (е-пошта, 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 заштитним зидовима, рутерима, прекидачима језгра и WiFi контролеру без конзоле 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;*

21. Заштита података у комуникационим мрежама укључујући уређаје и водове (3)

- Stateful or dynamic filtering (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, идентификатор скупа услуга (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 овлашћени саобраћај са бежичне мреже која користи безбедност Интернет протокола (ИПСец).
- **Ово захтева пуно времена за тестирање ако се у потпуности ради – то може бити посао за себе.**

Питања за 21. меру (1)

- Да ли су дефинисане и имплементиране network сецуриту манагемент процедуре?
- Да ли је имплементирано следеће :
  - Врсте контроле, као што су демилитаризоване зоне (DMZs)?
  - Сегментација мреже?
  - Proxy услуге?
  - Да ли је 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 инсталира мрежна компонента, а подразумеване лозинке укључујући SNMP низове су промењене у „јаке“ у свим заштитним зидовима, рутерима, кључним прекидачима и WiFi контролерима?

Питања за 21. меру (2)

- *Преглед скупова правила за заштитни зид и рутер се врши 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 у складу је са конфигурацијама заштитних зидова и рутера*?*
- Интерна мрежа је сегментирана и интерна мрежа је у свом сегменту мреже? DMZ је имплементиран да ограничи интернет долазни саобраћај само на ИП адресе и овлашћене јавно доступне сервисе (имејл, веб)?
- Нешифровани (небезбедни) протоколи као што су SSL, HTTP, Telnet, FTP, TFTP, SNMP v1 and v2, SSH нису коришћени у заштитним зидовима, рутерима, кључним прекидачима и WiFi контролерима или је документовано пословно оправдање за њихову употребу; Сав административни приступ заштитним зидовима, рутерима, прекидачима језгра и WiFi контролеру без конзоле је шифрован коришћењем јаке криптографије?
- *Заштитни зидови спречавају откривање приватних ИП адреса и рутирање информација са интерних мрежа на Интернет, на пример коришћењем НАТ-а?*
- *Да ли је принцип подразумеваног одбијања по коме се одбија сав саобраћај осим оног који је изричито захтеван имплементиран у правила заштитних зидова?*
- *Да ли се у заштитним зидовима имплементира филтрирање стања или динамичко (само „успостављене“ везе су дозвољене у мрежу)?*

Питања за 21. меру (3)

- *Да ли се примењују мере против лажирања (Anti-spoofing measures), на пример блокирање саобраћаја који потиче са Интернета са интерном изворном адресом?*
- *Само поуздане мреже и клијенти имају приступ VPN-у?*
- *Да ли су VPN везе обезбеђене употребом јаке криптографије?*
- *VPN везе су ограничене на неопходне сервере и услуге?*
- *Подељено тунелирање (Split tunneling) је онемогућено да би се спречило да потенцијални нападачи на дељеној мрежи компромитују удаљени рачунар и користе га за приступ интерној мрежи.*
- *Да ли је бежично умрежавање обезбеђено употребом јаке криптографије са WiFi Protected Access (WPA2)?*
- *Све фабричке поставке при инсталацији, укључујући, али не ограничавајући се на ИД-ове корисника администратора, лозинке/фразе на приступним тачкама, WPA кључ, идентификатор скупа услуга (SSID) и подразумеване низове SNMP заједнице, су промењене у „јаке“ приступне фразе?*
- *Периметарски заштитни зидови су инсталирани између свих бежичних мрежа и интерне мреже и дозвољавају само овлашћени саобраћај са бежичне мреже која користи безбедност Интернет протокола (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.
- Проверити 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 за 22. меру

- 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 конторла 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 за 23. меру

- Да ли је уређен интерни и екстерни развој пословних апликација?
- Да ли у су у захтеве за набавком пословних апликација укључени information security 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 укључене 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.
- (ISO 27002 контрола 14.3) - Тестирати - 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 окружењма 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 за 24. меру

- Да ли су приступна права подацима у тестним окружењма 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 VPN 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 за 25. меру

- 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 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.
- Проверити 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 за 26. меру

- 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 (1)

- 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.
- Проверити 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.

27. Превенција и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама (2)

- 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;
- Проверити 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;
- Проверити 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 за 27. меру (1)

- 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?

Питања за 27. меру (1)

- 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 (1)

- 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.

28. Мере које обезбеђују континуитет обављања послова у ванредним околностима (2)

- Проверити 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.
- Проверити да ли постоји IT disaster recovery план који обухвата сву опрему која подржава критичне процесе;
- Проверити 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 за 28. меру (1)

- Да ли је постоје мере којима се обезбеђује обављање послова у ванредним околностима?
- Да ли постоји BCP (Business Continuity Plan)?
- 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?

Питања за 28. меру (2)

- Да ли је урађена BIA (Business Impact Analysys)?
- Да ли су идентификовани сви критични процеси?
- Да ли су идентификовани RTO и RPO тих критичних процес?
- 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?

Провера ИКТ система

- Оператор ИКТ система је дужан да врши проверу ИКТ система, односно проверу усклађености примењених мера заштите са Актом о безбедности, мерама заштите прописаним Законом о информационој безбедности и Уредбом о мерама заштите.
- Провера може да се врши самостално или уз ангажовање спољних експерата.
- Провером се оцењује адекватност нивоа информационе безбедности путем провере мера заштите, процедура и одговорности утврђених актом о безбедности.
- Провером се утврђује угроженост или нарушавање информационе безбедности која настаје коришћењем неодговарајућих поступака и техничких средстава.
- Оператор ИКТ система је дужан да проверу врши најмање једном годишње и да о томе сачини извештај.

Провера се врши тако што се:

1. Проверава усклађеност Акта о безбедности ИКТ система, узимајући у обзир и акта на која се врши упућивање, са прописаним условима, односно проверава да ли су Актом адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему;
2. Проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима, методама интервјуа, симулације, посматрања, увида у предвиђене евиденције и другу документацију;
3. Врши провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система методом увида у изабране производе, архитектуре решења, техничке конфигурације, техничке податке о статусима, записе о догађајима (логове) као и методом тестирања постојања познатих безбедносних слабости у сличним окружењима.