UDC: 006.332:004.6.056 INFO M: str. 43-50

МЕРЕЊЕ ЕФЕКТИВНОСТИ СИГУРНОСНИХ КОНТРОЛА СИСТЕМА ЗА УПРАВЉАЊЕ СИГУРНОШЋУ ИНФОРМАЦИЈА КОРИШЋЕЊЕМ „ISO/IEC 27001“ СТАНДАРДА
USING „ISO/IEC 27001“ STANDARD FOR SECURITY CONTROLS EFFECTIVENESS MEASUREMENT IN INFORMATION SECURITY MANAGEMENT SYSTEMS

Ненад Милисављевић

РЕЗИМЕ: Циљ овог рада је да прикаже могућности примене „ISO/IEC 27001“ стандарда у процесу мерења ефективности сигурносних контрола које овај стандард прописује. У раду су, поред краћег историјског развоја и саме структуре стандарда, описани и потреба за мерењем ефективности сигурносних контрола, са циљем да се организацијама које примењују овај стандард омогући да сигурност информација третирају као мерљиви део свог пословања. У раду су, поред овога, дата и упутства по којима се ова мерења спроводе. На крају су, као додатак раду, за поједине контроле из стандарда „ISO/IEC 27001“ дати циљеви и механизми мерења ефективности успостављених сигурносних контрола, као и додатне информације о томе како се ова мерења могу користити за одређивање ефективности контрола са циљем успостављања компаративних и репродуктивних резултата.
КЉУЧНЕ РЕЧИ: ISO/IEC 27001, Систем за управљање сигурношћу информација, Мерење ефективности сигурносних контрола, Повраћај инвестиција
ABSTRACT: This paper deals with applying „ISO/IEC 27001“ standard in security effectiveness measurement process. The main objective of this paper is to give the brief description to organizations, that have already implemented „ISO/IEC 27001“ standard, on how to treat information security as a measurable part of its business line. This paper first introduces „ISO/IEC 27001“ standard, its historical development and its structure. Afterwards, this paper deals with needs for security effectiveness measurement and methods that can be applied. Several appendixes are given regarding objectives and measurement effectiveness mechanisms for certain „ISO/IEC 27001“ security controls. Additional information is also given regarding utilization of these measurements for controls effectiveness determination in order to establish comparable and reproducible results.
KEY WORDS: ISO/IEC 27001, Infromation Security Management System, Effectiveness measurement, Return of investments

1. УВОД

Савремено пословање је данас практично незамисливо без примене информационих технологија. Информације постају важан ресурс од кога практично зависи опстанак и развој читавих организација. Организације постају све отвореније повезујући своје информационе ресурсе са купцима, добављачима и осталим комитентима, што доводи до појаве бројних сигурносних претњи као што су рачунарске преваре, шпијунаже, саботаже, вандализми, пожари, поплаве и сл. Штете које настају у организацијама инфилтрирањем разних врста малициозних кодова, разне врсте рачунарског криминала и ускраћивања услуга су, нажалост, све присутнија појава.

Без обзира на облик у коме се чувају, информације морају бити адекватно заштићене. Да би се осигурала адекватна заштита информација сви корисници морају бити упознати са основним концептима сигурности информација и мерама заштите које они захтевају.

Заштита информација, очување њихове поверљивости, интегритета, односно целовитости и расположивости постаје од примарне важности. Сигурност информација је много више од коришћења одговарајућих техничких решења које нуде савремене информационе технологије. Јер као што је то наведено у књизи [1] „Ако мислите да технологијом можете решити ваш сигурносни проблем, онда ви не разумете ни проблем ни технологију“.

Ослањајући се на концепт да је сигурност информација много више од примене савремених техничких решења које нуде информационе технологије, развијени свет (пре свих Велика Британија, кроз своје национално тело за стандардизацију, „BSI“) определио се за развој одговарајућих стандарда који покривају ову област. Тако су средином деведесетих година прошлог века настали први стандарди „BS 7799–1“ и „BS 7799–2“ који су уређивали област сигурности информација. Развој ових стандарда је од две хиљадите године преузела Међународна организација за стандардизацију („ISO“), заједно са Међународном електротехничком комисијом („IEC“) кроз заједнички технички комитет („JTC1“).

Следећи ово, у овом раду је представљен концепт мерења ефективности успостављених сигурносних контрола коришћењем стандарда „ISO/IEC 27001“.

2. „ISO/IEC 27001“ СТАНДАРД

Стандард „ISO/IEC 27001“ описује процесе успостављања и управљања системима за управљање сигурношћу информација (енгл. „Information Security Management System”, или скраћено „ISMS“).

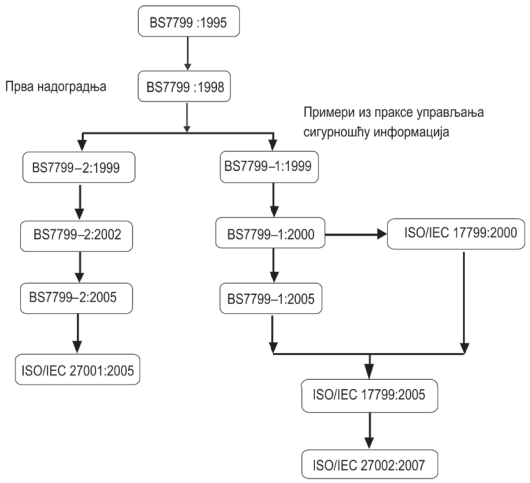
Систем за управљање сигурношћу информација може се једноставно протумачити као скуп сигурносних мера којима се смањују могућности нападача, независно од тога да ли се ради о екстерном или интерном нападачу. Систем за управљање сигурношћу инфомација је истовремено и средство помоћу којег највише руководство организације прати и надзире сигурност информационих система организације, сводећи тако пословни ризик на минимални ниво и осигуравајући на тај начин да ће сигурносни захтеви пословања испунити све корпорацијске и правне обавезе.

Стандард „ISO/IEC 27001“ пружа систематски приступ управљању осетљивим информацијама са циљем очувања њихове сигурности. Основни циљ овог стандарда је постизање сигурности информација у три главна аспекта: поверљивост, интегритет и расположивост, узимајући при томе у обзир и релевантне ресурсе, политике, процедуре и информационе системе.

2.1. *РАЗВОЈ „ISO/IEC 27001“ СТАНДАРДА*

Прву верзију „ISO/IEC 27001“ стандарда донела је Велика Британија 1995.године, а овај стандард је носио назив – „BS 7799“. Овај иницијални стандард се касније мењао 1999/2000. године, а након тога и 2002. и 2005. године. Међународна организација за стандардизацију, „ISO“, као кровна организација, већину стандарда преузела је из британских модела стандарда. Данас се још увек, упркос постојању „ISO“ стандарда, у разговорима може чути о „BS 7799“ стандарду као зачетнику сигурносних правила и процедура (Слика 1). Стандард „ISO 27001:2005“ усвојен је као међународни стандард 15.10.2005. године.

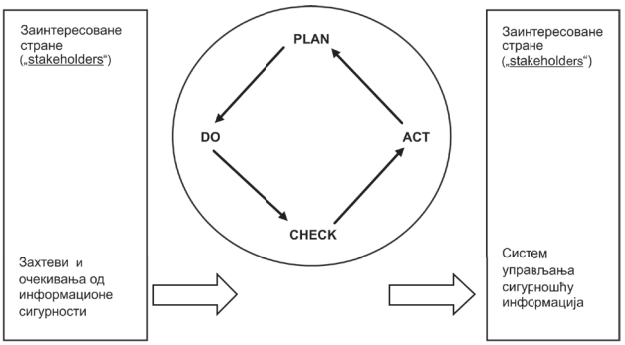
„ISO/IEC 27001:2005“ стандард припремила је заједничка комисија „Joint Technical Committee ISO/IEC JTC 1, Information Technology, Subcommittee SC 27, IT Security techniques“ (Заједнички технички комитет „ISO/IEC“ за информационе технологије, подкомитет „SC 27“ за безбедносне технике информационих технологија).



Slika 1. – *Историјат „ISO 27001“ и „ISO 27002“ стандарда*

2.2. *СТРУКТУРА „ISO/IEC 27001“ СТАНДАРДА*

„ISO/IEC 27001“ стандард употребљава „PDCA“ (енгл. „Plan–Do–Check–Act“) модел управљања сигурношћу информација. Овај модел истиче важност пажљивог планирања имплементације система, што за резултат има ефикасне мере за његово трајно побољшање и правилну употребу. „PDCA“ модел је приказан на слици 2.



Slika 2. – *„PDCA“ модел примењен на системе за управљање сигурношћу информација*

Tabela 1– Опис активности укључених у појединачне фазе „PDCA“ циклуса

ФАЗА	ОПИС АКТИВНОСТИ
„Plan“ (Успоставити систем за управљање сигурношћу информација)	Успоставити политику система за управљање сигурношћу информација, циљеве, процесе и процедуре важне за управљање ризиком и повећање сигурности информација, како би достигли резултате који су у складу са укупном политиком и циљевима организације.
„Do“ (Имплементирати систем за управљање сигурношћу информација)	Имплементирати и извршавати политике, контроле, процесе и процедуре система за управљање сигурношћу информација.
„Check“ (Надгледати и проверавати систем за управљање сигурношћу информација)	Проценити и, где је применљиво, мерити перформансе процеса у односу на систем за управљање сигурношћу информација, и извештавати менаџмент о резултатима.
„Act“ (Одржавати и побољшавати систем за управљање сигурношћу информација)	Предузети корективне и превентивне мере засноване на резултатима интерног надзора система за управљање сигурношћу информација, како би се омогућило континуирано побољшање система за управљање сигурношћу информација.

У следећој табели (Табела 1.) налази се опис активности укључених у појединачне фазе „**PDCA**“ циклуса.

2.3. *ИНТЕГРАЦИЈА „ISO/IEC 27001“ СТАНДАРДА СА ДРУГИМ СТАНДАРДИМА*

„ISO 27001“ стандард је припремљен на такав начин да се одлично интегрише са пословним процесима организације, као и са већ постојећим стандардима „ISO 9001“ и „ISO 14001“, те се кроз призму пословне оправданости управља процесима информационе сигурности у организацији. Овај стандард је врло добро прихваћен јер осигурава флексибилност, дефинише управљачки оквир, а при том не задире у конкретну техничку имплементацију, што га чини релативно лако применљивим у различитим организацијама.

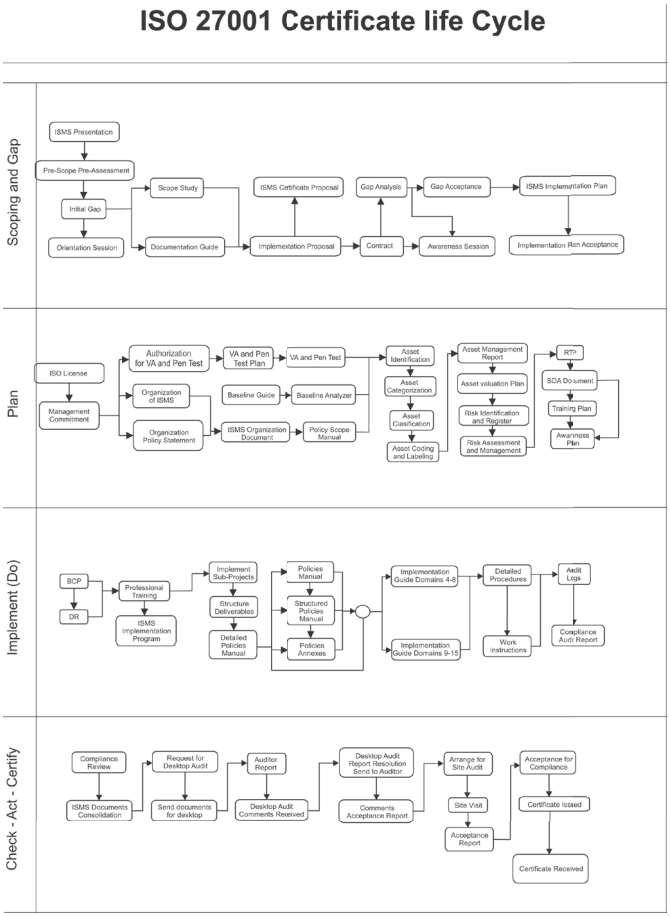
Заједно уз „ISO 27001“ стандард готово увек се помиње и „ISO 27002:2007“ стандард (који је раније носио назив „ISO 17799:2005“), и који је као скуп препорука и смерница израђен према најбољој пракси из своје области. „ISO 27001“, као кровни документ, садржи попис захтева обавезних за сертификацију и директно се референцира на „ISO 27002“ стандард, као скуп смерница и контрола које је потребно имплементирати приликом успостављања система за управљање сигурношћу информација.

Такође, када се говори о стандардима у области безбедности и заштите података, обавезно се мора навести и „Payment Card Industry Data Security Standard“ (скраћено „PCI DSS“), који данас заузима све значајније место у системима за рад са платним картицама [2]. Овај стандард је настао 15.12.2004. године, а издао га је Савет за индустријске стандарде сигурности платних картица (енгл. „Payment Card Industry Security Standards Council“, или скраћено „PCI SSC“). Овај стандард је настао практичним спајањем више стандарда који су покривали област безбедности података током прошле декаде. Међу овим стандардима се налазе и: „BS7799“ стандард; „ISF“ стандарди односно стандарди добре праксе (енгл. „Standard of Good Practice“) (које је издао „Information Security Forum“), „Basel II“, „Gramm–Leach–Bliley Act (GLBA)“, „Health Insurance Portability and Accountability Act (HIPAA)“, као и „Sarbanes–Oxley Act“ из 2002. [3].

„PCI DSS“ стандард се не разликује драстично од захтева које поставља „ISO/IEC 27001“ стандард, нарочито ако се има у виду чињеница да оба стандарда покривају сегменте који припадају области заштите података и да су оба стандарда настала из истог – „BS7799“ стандарда. Ови стандарди се чак и преклапају у неким својим деловима. Међутим, постоји и неколико разлика између ових стандарда. Највећа разлика између ових стандарда је у томе што „PCI DSS“ стандард не захтева предуслове за успостављање система за управљање сигурношћу информација, као што је нпр. посвећеност менаџмента; док са друге стране стандард „ISO/IEC 27001“ налаже успостављање већег броја процеса, али истовремено не залази у детаље везане за начине имплементације неопходних контрола. Друга, веома битна разлика између ових стандарда, лежи у чињеници да иако „ISO/IEC 27001“ стандард прописује одређени сет контрола (прецизније 133 контроле), он од организација које се са њим усклађују не захтева експлицитну усклађеност са свим контролама, што није случај са „PCI DSS“ стандардом који експлицитно захтева усклађивање са свим контролама које се налазе у стандарду.

2.4. *ЖИВОТНИ ЦИКЛУС СЕРТИФИКАЦИЈЕ ПРЕМА „ISO/IEC 27001“ СТАНДАРДУ*

На следећој слици (Слика 3.) дат је преглед свих корака које је потребно предузети у организацији приликом имплементације система за управљање сигурношћу информација и сертификације компаније у складу са истим:



Slika 3. – *Животни циклус процеса сертификације компаније у складу са „ISO 27001“ стандардом*

Такође, као прилог овом раду у додатку „Д“ овог рада се налази преглед комплетне документације „ISMS“ чије постојање прописује стандард „ISO 27001“.

3.МЕРЕЊЕ ЕФЕКТИВНОСТИ СИГУРНОСНИХ КОНТРОЛА КОРИШЋЕЊЕМ „ISO/IEC 27001“ СТАНДАРДА

Иако се циљеви и сама суштина стандарда „ISO/IEC 27001:2005“ не разликују драстично од истих у стандарду „BS 7799–2:2002“, који је представљао његову претечу, ипак постоји једна суштинска разлика, а то је захтев за

мерењем ефективности изабраних контрола приликом имплементације овог стандарда (за више детаља „ISO/IEC 27001:2005“ клаузула „4.2.2 d“). Овај захтев је специфичан и по томе што не само да одређује начин на који ће се мерење ефективности контрола извршити, већ и по томе што уређује да ове метрике морају бити упоредиве и репродуктивне, односно да се резултати добијени њиховом применом могу упоређивати, као и то да се ове метрике могу више пута користити.

Ово на први поглед може изгледати прилично једноставан задатак, с обзиром да већина „ИТ“ сектора у компанијама већ спроводе неке врсте метрика (на пример „KPI“ (скраћено од енгл. „Key performance indicator“); „ITIL“ ... и др.), па је из тог разлога логично мерити и ефективност успостављених сигурносних контрола, како би се свим „stakeholder“–има могла приказати ефективност ових контрола, на основу чега се даље може проценити и оправданост новца уложеног у њихову имплементацију. Нажалост, с обзиром да се ради о сигурности, ово и није баш толико једноставно извести колико се то на први поглед можда може учинити да јесте. На срећу, у организацијама се у пракси често наилази на већ адекватно имплементиране сигурносне контроле (нарочито у оним организацијама које су већ имплементирале „Cobit“, „ITIL“ или „BS 7799“ стандард). Примери овога су адекватне анти–вирусне политике или добра физичка заштита. У оваквим случајевима проблеми настају када се дубљом анализом дође до тога како су, на који начин и због чега баш ове контроле изабране и како ће бити мерена њихова ефикасност.

Највећи јаз обично настаје у вези документације, која би требала да објасни везу између идентификованих ризика и противмера које су предузете због којих су оне предузете. Овај јаз често потиче из неразумевања праве суштине оригиналног „BS 7799:1999“ стандарда – управљања ризицима.

У пракси су честе ситуације да се организације приликом имплементације стандарда толико фокусирају на то да обезбеде имплементацију свих контролних циљева (у ранијем стандарду их је било 127) и да их наведу у Изјави о применљивости (енгл. „Statement of Applicability“, скр. „SoA”), да једноставно „забораве“ да успоставе везу између ризика којима је организација изложена и система за управљање сигурношћу информација (скр. „ISMS“).

Пример овог проблема, који се у пракси често среће, јесте случај да неке компаније које су изабрале да имплементирају, рецимо, скупи систем за детектовање спољних напада (енгл. „Intrusion Detection System“, скр. „IDS“), не знају баш увек како су и зашто дошли на идеју да га уопште имплементирају. С обзиром на ово, веза између ризика и трошка инвестиције најчешће није ни разматрана, па се самим тим није ни разматрало мерење ефективности имплементираног „IDS“. Поред овога, још више забрињава ситуација да је само мали проценат компанија разматрао повратак инвестираних средстава.

С обзиром на ово, логично се намећу питања у вези тога које је контроле потребно мерити, као и то како се ови резултати могу искористити за осигурање да све имплементиране сигурносне контроле ефективно функционишу?

Још један разлог зашто је ово једна од горућих тема је и то што су се водећа тела за стандардизацију, као што су „BSI“ и „ISO“, такође заинтересовала за наведени проблем. Ове организације теже томе да успоставе синергију између „ISO 20000“, „ITIL“ и „ISO 9001“ стандарда, како би пронашли сет мера које се лако могу повезати са постојећим или новим системима за управљање.

С обзиром на све до сада изнето, поставља се питање одакле треба почети? Најједноставније би било рећи да је потребно само имплементирати сет контрола које прописује „ISO 27001“ стандард, а које се базирају на процењеним ризицима, са циљем да ове контроле обезбеде ублажавање, трансфер или једноставно елиминацију идентификованих ризика. Међутим, није све тако једноставно. Систем за управљање сигурношћу информација требало би да имплементирају експерти, који разумеју ризике, као и важност коришћења адекватних контрола. Добар основ за грађење доброг система за управљање сигурношћу информација представљају потпуно документоване, испробане и тестиране процедуре за управљање инцидентима, комплетне процедуре за праћење и ревидирање рада у оквиру ИС, и, изнад свега овога, јасна стратегија које метрике ће се користити за мерење ефективности сигурносних контрола.

3.1. *ПОТРЕБА ЗА МЕРЕЊЕМ ЕФЕКТИВНОСТИ СИГУРНОСНИХ КОНТРОЛА*

Мерење ефективности имплементираних сигурносних контрола треба да задовољи следеће циљеве:

- Да јасно приказује текућа побољшања у односу на претходно стање;
- Да прикаже усклађеност пословања организације са свим стандардима, уговорима, законским одредбама и свим другим потребним актима;
- Да оправда будуће трошкове (нови сигурносни софтвер, обуке, нове кадрове, ...);
- Да идентификује места где имплементиране контроле нису ефективне и не задовољавају постављене циљеве;
- Да увери највиши менаџмент, као и све друге „stakeholder“–е у ефективност имплементираних контрола;
- И на крају, то захтева „ISO 27001“ стандард, као и други стандарди за управљање пословањем („ISO 9001“, „ISO 20000“, ... и др.).

Поред овога, мерење сигурности доноси и одређене предности организацијама које овај процес спроводе, што ће рећи:

- Олакшава процесе праћења ефективности „ISMS“ ;
- Проактивним алатима за мерење се могу спречити касније ескалације проблема (на пример, уска грла на

рачунарској мрежи, неуређене податке на дисковима, ... и др.);
– Смањује број сигурносних инцидената;
– Представља јасно видљиве доказе ревизорима, као и осигурање вишем менаџменту да се запослени адекватно контролишу у области заштите података.

Из овога видимо да, без обзира на то шта је иницијално био циљ за имплементацију „ISMS“ коришћењем „ISO 27001“ стандарда, након имплементације овај циљ више не треба да буде само скуп контрола које је потребно одабрати и имплементирати, већ и како ће те контроле касније бити мерене. Уколико се оне не могу измерити, како се уопште може знати да ли оне раде ефективно или не? Суштина овога је да ће све организације ускоро моћи да третирају сигурност као мерљиви део пословања (са циљем базирања на најбољим примерима из праксе или на „ISO 27004“ стандарду, који ће се бавити искључиво метрикама информационе сигурности, а чији је развој тренутно ушао у трећу фазу, односно израду драфт верзије стандарда).

3.2. *МЕРЕЊЕ ЕФЕКТИВНОСТИ СИГУРНОСНИХ КОНТРОЛА*

Ради лакшег праћења ефективности контрола, контроле је потребно поделити у 4 велике групе, и то:

– Управљачке контроле:
  o Сигурносна политика, ИТ политике, Сигурносне процедуре, Планови за обезбеђења континуитета пословања, Планови за унапређење сигурности, Пословни циљеви, Прегледи од стране менџмента
– Пословне процесе:
  o Процене ризика и процесе третирања и управљања ризицима, Процесе „HR”, Процес одабира „SoA“, Процес руковања медијумима
– Оперативне контроле:
  o Оперативне контроле, Контроле измена, Управљање проблемима, Управљање капацитетима, „Back up“, Размештај рачунарске опреме на више локација
– Техничке контроле:
  o Управљање ажурирањем системског софтвера, Анти–вирусне контроле, „IDS“, „Firewall“, Филтрирање садржаја и саобраћаја.

Дакле, мерење се може вршити према:

– Делимичним сигурносним контролама или циљевима;
– Групама контрола;
– Према контролама које се налазе у стандарду;
– Према неком од примера који ће бити описани у наставку рада

Даље се процес мерења ефективности сигурносних контрола (група контрола) наставља кроз следеће кораке:

– Потврду релевантности контрола кроз процену ризика;
– Дефинисање циљева и обезбеђење да они заиста осликавају стварну потребу пословних циљева;
– Успостављање нових и коришћење постојећих индикатора где год је то могуће (на пример у „ITIL“ условима то би били кључни индикатори перформанси (енгл. „Key Performance Indicators“ или скраћено „KPI“));
– Спровођење ревизије опсега важења „ISMS“, у оквиру које је потребно идентификовати контроле које се могу непрекидно пратити коришћењем одабране технике;
– Постављање основних начела за сва будућа мерења, које је потребно упоређивати са претходним;
– Обезбеђење креирања периодичних извештаја према надлежном менаџменту / власницима „ISMS“ (укључујући графичке приказе, слике и др.);
– Идентификовати критичну полазну основу – прихваћене препоруке, корективе радње и сл;
– Имплементирати побољшања у Интегрисани систем за управљање (енгл. „Integrated Management System“; или скр „IMS“) на пример „ISO“ стандарде „9001“, „14000“, „27001“, „20000“ и др.;
– Имплементирати „PDCA“ приступ („Plan–Do–Check–Act“) управљања у „ISMS“.

Мерење ефективности сигурносних контрола свакако мора да задовољи и одређене услове, односно:

– Да пресликава пословне циљеве организације;
– Мора бити критично према успешним операцијама;
– Мора бити мерљиво, репродуктивно (односно да се више пута може изводити) и упоредиво;
– Мора олакшавати корективе акције;
– С обзиром да свако мерење захтева дефиницију, онда свако мерење треба и да обезбеди да се следећа листа користи за сваку дефиницију:
  o Назив мерења;
  o Опсег метрика;
  o Намену и циљеве мерења;
  o Методе коришћене за мерење;
  o Фреквенцију мерења;
  o Процедуре извора и колекција података;
  o Одабране индикаторе;
  o Датуме мерења и одговорне особе;
  o Постигнути ниво измерене ефективности;
  o Узроке евентуалног неуспеха мерења.

4.ЗАКЉУЧАК

Као што се из овог рада може видети, сви „ISMS“, сертификовани према „ISO 27001“ стандарду, без обзира на њихову величину, очекују и захтевају извршавање макар основних мерења њихове ефективности. У супротном, било би немогуће доказати било која побољшања која су направљена или чија је корекција захтевана.

Такође је веома важно обезбедити да се сва мерења редовно записују, односно да се о њима води ажурна евиденција (на пример, у „excel“ табелама или на неки сличан начин), како би се контроле које се мере касније могле упоређивати са новим резултатима. На овај начин се олакшава и каснија припрема разних статистичких анализа (презентације / извештаји за највиши менаџмент у вези израчунатог очекиваног губитка, повратка инвестираних средстава и сл.).

У овом раду је:

- наглашена потреба мерења ефективности „ISMS“, као и предности које из таквог приступа произилазе;
- дат приказ најчешћих грешака које се у пракси јављају приликом успостављања „ISMS“;
- описан начин на који се стандард „ISO 27001“ може користити за мерење ефективности контрола успостављених у „ISMS“, и дати су адекватни примери.

Као додатак овом раду урађени су примери начина на који се могу извршити мерења појединих контрола прописаних „ISO 27001“ стандардом, подељених, према функционалностима, у четири групе контрола: Управљачке контроле, Пословне процесе, Оперативне контроле и Техничке контроле (Ови прегледи се налазе у додацима „А“, „Б“, „В“ и „Г“ овог рада). Такође, у додатку „Д“ , налази се и списак комплетне документације „ISMS“ чије постојање прописује стандард „ISO 27001“.

Додатак „А“ – Управљачке контроле

Референтна група контрола	Референца у ISO 27001 стандарду	Назив	Појашњење и циљеви мерења	Циљеви мерења, механизми	Како се ова мерења могу користити за одређивање ефективности контрола са циљем успостављања компаративних и репродуктивних резултата
Клаузула 4	4.2.1	Ефективна сигурносна политика	Објашњавање важности испуњавања циљева информационе сигурности и поштовање сигурносне политике, њених одговорности пред законом и потребом за континуалним побољшањем.	Ефективност се мери кроз успешност иницијално прописаног, а затим се врше периодични прегледи, два пута годишње.	Мерењем доступности и распрострањености сигурносне политике, њеним познавањем и разумевањем. Мерења се могу спровести интервјуисањем насумично одабраних запослених на тему познавања и разумевања сигурносне политике.
	4.2.1	Сет документације за „ISMS“ (може се погледати у додатку „Д“, који се налази као додатак овом раду)	Узети тренутни статус (изражен у %) политика и процедура које подржавају „ISMS“	Мерењем комплетне документације до краја прве године треба достићи циљ од 90%; затим 95% у другој години, док у трећој години циљ треба бити комплетна документација - 100%.	Редовни годишњи прегледи целокупне документације „ISMS“ требају да обезбеде константно испуњење задатих циљева и да обезбеде упоредљивост са резултатима постигнутим у претходној години.
Клаузула 7	7.2; 7.3; A.6.1.1	Улазни и излазни подаци за преглед „ISMS“ од стране менаџмента	Менаџмент мора годишње да проверава „ISMS“ и сву пратећу документацију прописану „ISO 27001“ стандардом (додатак „Д“ овог рада). Као додатна активност се менаџменту поставља и преглед метрика изабраних да обезбеде да су побољшања адекватно успостављена и да ефикасно функционишу.	Улазни подаци на основу којих би требало да се базира преглед „ISMS“ од стране менаџмента би требали да укључе резултате мерења ефективности. Излазни подаци овог прегледа би требали да сардже све одлуке и акције које су на било који начин повезане са побољшањем функционисања начина мерења ефективности контрола.	Сваке године би преглед требао да укључи резултате прегледа од претходне године како би се обезбедило да се слични налази не понављају, или барем да не остају нерешени, чиме би се обезбедили видљиви докази компарабилних резултата.
A.15	A.15.1.2	Ефективна техничка мерења и мерења сигурносних политика	% „IT“ система усклађених са сигурносним политикама и стандардима, треба у првој години да достигне циљ до 50%; затим 75% у другој години, док у трећој години циљ треба да достигне усклађеност од 95% система.	Мерењем кроз % контролних ИТ сигурносних тачака и серије извршених ИТ ревизија у току године.	Број контролних тачака би требао да почне да се стабилизује након друге године. Проценат откривених могућности за унапређење би требао да опада током трогодишњег периода. До краја прве године би требао да буде =<90%, до краја друге године би требао да буде =<80%, а до краја треће године би требао да буде =<70% откривених.
	A.15.1.2	Ефективна сигурносна политика	Додатна обука и чести тестови запослених у погледу разумевања десет највише рангираних сигурносних ризика са којима се организација сусреће	% запослених који су прошли обуку треба на крају прве године да достигне ниво до 50%, до краја друге године ниво до 80%, док на крају треће године овај ниво треба да буде 99%.	% испитаних запослених путем упитника се повећава сваке године у односу на претходну. % тестираних испитаника побољшава своје резултате годину за годином.

Додатак „Б“ – Пословни процеси

Референтна група контрола	Референца у ISO 27001 стандарду	Назив	Појашњење и циљеви мерења	Циљеви мерења, механизми	Како се ова мерења могу користити за одређивање ефективности контрола са циљем успостављања компаративних и репродуктивних резултата
„SoA“ (Изјава о применљивости)	4.2.1.j	Изјава о применљивости (Statement of Applicability)	1) контролни циљеви и контроле, наведени у одељку „4.2.1.g“ и разлози њиховог одабира; 2) контролни циљеви и контроле тренутно имплементирани („4.2.1.e“); 3) искључење било ког контролног циља из Анекса А „ISO 27001“ стандарда и разлог за његово искључивање.	Применљивост сваке контроле се годишње проверава како би се обезбедила њена прикладност.	% прецизности треба да се одржава на нивоу вишем од 95% сваке године и треба га упоређивати са процентом прецизности од претходне године.
Процена ризика и управљање ризицима	4.2.1.d,e,f,g	Процена ризика, Процес третирања ризика и Регистар ризика	Контролни циљеви требају бити селектовани и имплементирани да задовоље захтеве идентификоване у процесима процене ризика и третирања ризика (укључујући при томе и ажурирање регистра ризика)	Сви ризици требају бити уграђени у централизовани регистар ризика, док се одређени број ризика треба идентификовати и њима управљати у оквиру специфицираног временског периода, односно времена потребног за одговор на ризик.	Статистичке анализе се требају користити за графичку презентацију управљања ризицима и за број ризика којима се не управља, при чему број таквих ризика којима се не управља треба да остане испод одређене доње границе.
Третирање ризика	Клаузула 8	Планови за третирање ризика	Формулисати план за третирање ризика који идентификује одговарајуће акције менаџмента, ресурсе, одговорности и приоритете за управљање ризицима информационе сигурности.	Третирање ризика је једно од основних начела информационе сигурности, па стога мерење ефективности треба да обезбеди да се резултати периодично прегледају и побољшавају.	Број критичних системских ризика, према спроведеној анализи ризика, треба да буде једнак „X“. До краја прве године (од успостављања „ISMS“) овај број треба да буде мањи од „X“, а до краја друге године овај број треба да буде „X/2“.

Додатак „В“ – Оперативне контроле

Референтна група контрола	Референца у ISO 27001 стандарду	Назив	Појашњење и циљеви мерења	Циљеви мерења, механизми	Како се ова мерења могу користити за одређивање ефективности контрола са циљем успостављања компаративних и репродуктивних резултата
A.10	A.10.1 Оперативне процедуре и одговорности	Обезбеђивање тачних и сигурних операција приликом њиховог процесирања	Потврда да ли одговарајуће процедуре обезбеђују сигурност основних средстава организације, да ли задовољавају све потребе „ISMS“, као и да ли се сви послови релевантни за пословање организације документују.	Мерења се могу спровести или коришћењем документ менаџмент система, или коришћењем докумената који садрже процедуре повезане са њима, или потенцијално осетљивих делова „ISMS“ (на пример процедура за „Back up“ или слично).	Годишње ревизије и број инцидената ће показати да ли овакве контроле раде и да ли се ефективно користе, или не. Докази: - Годишње ревизије система за управљање квалитетом и/или документ менаџмент система; - Број захтева за умањење важности, одобрених од стране менаџера за сигурност; - Преглед сегрегације дужности (као део процеса ревизије)
A.10.3	A.10.3 Планирање и прихватање система	Умањивање ризика од непредвиђених падова система	Планирање и прихватање система треба бити контролисано управљањем конфигурисањем система, контролама увођења измена на систему и техникама планирања капацитета.	Број система / процеса који потпадају под ове контролне механизме ће детерминисати која мерења и у којој мери се могу применити.	Годишње ревизије и број система који је квалификован за овакве контроле треба да се повећава. Ово представља индикатор да ли имплементиране контроле функционишу и да ли се ефикасно користе. Докази: - Резултати ревизија потврђују да ли је управљање изменама на систему, управљање конфигурисањем и планирање капацитета у оперативној функцији или није. Број неусклађених налаза сваке године треба да се смањује у односу на претходну.
A.10.5	A.10.5 Back-up	Развој интегритета и доступности информација и опреме за њихово процесирање	Да ли су процедуре за Backup у складу са вишим политикама и процедурама мериће се у односу на сигурносну политику.	Циљ овог мерења је да обезбеди да се процедуре за Backup обављају координисано и у складу са најбољом праксом која се на дату организацију може применити. Ово мерење треба да помогне у идентификовању потенцијалних ризика који се могу јавити при покушају поновног учитавања пређашњег стања са „Back up“–а.	Ефективност ће се мерити у односу на то да ли је политика за „Back up“ примењена у свим релевантним областима које су идентификоване као оне које захтевају редован „Back up“. Докази: - Резултати ревизија

Додатак „Г“ – Техничке контроле

Референтна група контрола	Референца у ISO 27001 стандарду	Назив	Појашњење и циљеви мерења	Циљеви мерења, механизми	Како се ова мерења могу користити за одређивање ефективности контрола са циљем успостављања компаративних и репродуктивних резултата
A.12	A.12.6.1	Доступност опреме за управљање ажурирањем системског софтвера	Провера да ли систем за управљање ажурирањем системског софтвера обезбеђује сигурност основних средстава организације, да ли задовољава све потребе „ISMS“, као и то да ли се сви послови релевантни за пословање организације документују.	Број система/процеса који потпадају под ове контролне механизме ће детерминисати која мерења и у којој мери се могу применити	Уколико % система који се налазе под централним системом за управљање ажурирањем системског софтвера на почетку износи „Z“, онда до краја прве године овај % треба да буде већи од „Z“, и тако редом сваке године, са константним повећањем.
A.10	A.10.10.3	Доступност коплетних „log“ фајлова опреме / приступ сигурносним информацијама у „log“ фајловима	Доступност информација из „log“ фајлова, као и процес њиховог прикупљања помаже приликом утврђивања да ли су успостављени процеси адекватни и да ли функционишу ефикасно, или не.	Број система/процеса који потпадају под ове контролне механизме ће детерминисати која мерења и у којој мери се она могу применити	До краја прве године се требају успоставити такви системи („IDS“ и/ или лог фајлови) за праћење да ће се на крају године пратити сви критични сервиси.
A.8	A.8.3.3	Време потребно за укидање корисничког налога	Време потребно за укидање налога из система показује колико добро се контролише приступ информационом систему.	Број система/процеса који потпадају под ове контролне механизме ће детерминисати која мерења и у којој мери се могу применити	Уколико је просечно време потребно за укидање налога „W“, онда оно до краја прве године мора да буде мање од „W“ и тако даље са константним смањењем сваке године.

Додатак „Д“ – Обавезна документација приликом успостављања „ISMS“

„ISO 27001“ налаже обавезно успостављање следећег сета документације [4]:

– Кровна сигурносна политика
– Опсег важења (енгл. „Scope“),„ISMS“;
– „ISMS“ / „ISO 27001“ Иницијална пројектна документација;
– „ISMS“ Оперативни приручник (енгл. „Operational Manual“) (Организациони дијаграми и структуре за извештавање);
– Улоге и одговорности у „ISMS“ (спонзори и власници пројекта ... и сл.);
– Форум за информациону сигурност („Terms of reference“);
– Регистар информационе имовине (у коме је потребно навести целокупну критичну пословну имовину која је повезана са ИТ);
– Методологију процене ризика и План за управљање ризицима (као и све политике и процедуре);
– Програм за унапређење сигурности (Укључујући резултате процене ризика, резултете спроведених ревизија ... и сл.);
– Техничке ИТ сигурносне политике (на пример, политика развоја софтвера, антивирусна политике ... и сл.);
– Сигурносне особине ИТ система (на пример, сигурносну мрежну топологију, политику приступа ... и сл.);
– Програм кампање сигурносне обуке (енгл. „Security Awareness Campaign Programme“) (пројектни план са циљевима);
– Изјава о применљивости (енгл. „Statement of Applicability“);
– Политика и оквир сигурносних ревизија;
– Процедуре и распоред ревизија – повезаност са системом за управљање квалитетом;
– Процедуре за управљање инцидентима, истраживањама и испоруком одговарајућих решења;
– Политике и процедуре за праћење и логовање рада корисника
– Политике и процедуре чувања података;
– „BCP“ и „Disaster recovery“процедуре

ЛИТЕРАТУРА:

[1] Humphreys T., Plate A., “An International Common Language for Information Security”, ISMS Journal, Issue 6, Jan 2006;
[2] Simić Dejan – „Proces primene PCI standarda“, INFO M 31/2009 str. 19–24, UDC: 004.738:336.7
[3] http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard ; октобар 2009
[4] International standard ISO/IEC 27001:2005; Information technology — Security techniques — Information security management systems – Requirements;

Ненад Милисављевић, дипл. инж., IT ревизор,
Комерцијална Банка А.Д. Београд
e–mail: nenad.milisavljevic@kombank.com
Области професионалног интересовања: Обезбеђивање сигурности информационих система и поверљивости података, Управљање ризицима информационе сигурности, IT ревизија, сет „ISO 27000“ стандарда

CIP - Katalogizacija u publikaciji Народна библиотека Србије, Београд 659.25
INFO M: časopis za informacionu tehnologiju i multimedijalne sisteme = journal of information technology and multimedia systems
glavni i odgovorni urednik Dragana Bečejski Vujaklija. . - . –
Beograd : Fakultet organizacionih nauka,
2002- (Stara Pazova : SAVPO). - 30 cm
- Tromesečno ISSN 1451-4397 COBISS.SR-ID 105690636