УНИВЕРЗИТЕТ „ГОЦЕ ДЕЛЧЕВ“ – ШТИП
ФАКУЛТЕТ ЗА ИНФОРМАТИКА
Информациони системи и технологии

Александар Арсовски

КОМПАРАТИВНА АНАЛИЗА И ДЕТАЛЕН ПРИКАЗ НА ПРОЦЕСОТ НА СЕРТИФИКАЦИЈА НА ИНФОРМАЦИСКИ СИСТЕМИ ВО ДРЖАВНИТЕ ИНСТИТУЦИИ НА РЕПУБЛИКА МАКЕДОНИЈА

МАГИСТЕРСКИ ТРУД

Штип, април 2017

Комисија за оценка и одбрана

Претседател : Проф. Зоран Здравев

Ментор : Проф. Александра Милева

Член : Проф. Доне Стојанов

Научно поле : 110 Информатика
Научна област : 11000 Информатика

Датум на одбрана : 12.04.2017
Датум на промоција :

СОДРЖИНА

Листа на слики

Листа на табели

Рецензирани и објавени трудови

1. Arsovski, Aleksandar and Mileva, Aleksandra (2015) *Анализа на процесот на сертификација на информациските системи на државните органи во Република Македонија согласно Законот за електронско управување.* Yearbook of the Faculty of Computer Science, 4 (4). pp. 63-70. ISSN 1857- 8691

Резиме

Во изминатите 30 години примената на современи технологии и нови практики овозможува зголемена продуктивност и подобра комуникација во работните организации. Организациите и компаниите за да ги подобрат своите услуги воспоставуваат информациони системи. Информациониот систем претставува комбинација од софтвер, хардвер и човечки ресурси кои се користат за поефикасно да се обработуваат и споделуваат саканите податоци. Но со постојаното подобрување на услугите се соочуваме и со поголеми предизвици за непрекинато функционирање на услугите кои ги нудиме. Сигурносните закани и проблемите поврзани со истите претставуваат едни од позначајните предизвици.

Со цел успешно справување со безбедносните ризици, во Република Македонија е усвоена законска рамка претставена во збир на минимални препораки. Оваа рамка која е задолжителна за државните органи е утврдена во Законот за електронско управување каде е пресликана во процес на сертификација на информационите системи. Покрај сертификацијата опфатена во законот како задолжителна за државните институции, постои и т.н. интернационална рамка која опфаќа мноштво на стандарди или методологии како на пример *ITIL, COBIT* , *ISO* сертификација и други. *ISO* сертификацијата и *COBIT* се доброволни и може да се применуваат во сите организации вклучувајќи ги и државните органи. Доколку се применува ваков вид на сертификација од државните органи истата треба да е лесна за имплементација и ускладена со легислативата во Република Македонија, односно во голема мера да соодветствува со стандардите барани согласно Законот за електронско управување и подзаконските акти.

Во повеќето организации може да се сретнат голем број на безбедносни мерки за заштита на своите податоци. Сепак без воспоставен структуриран систем за менаџмент со информационата безбедност, контролата може да биде неорганизирана, неефикасна и специфицирана само за одреден број на случаи. *ISO/IEC 27000* фамилијата од стандарди претставува збир на стандарди за систем за менаџмент на информациона безбедност, објавени од Меѓународната организација за стандарди (анг. *International Organization for Standardization - ISO*) и Меѓународната електротехничка комисија (анг. *International Electrotechnical Commission - IEC*). *COBIT* методологијата, пак, е креирана од *ISACA (Information Systems Audit and Control Association)* и *ITGI (*анг. *IT Governance institute)* и цели кон обезбедување збир од добри меѓународни практики за темелен, структуриран и стандардизиран процес кој важи за сите области не само за ИТ. Стандардите претставуваат рамка на политики и процедури кои ги вклучуваат сите правни, физички и технички контроли во процесот на менаџирање на информациониот ризик во организацијата.

ISO/IEC 27001 содржи препораки за најдобри практики за менаџмент со информациона безбедност, ризици и контроли во контекст на еден севкупен систем за менаџирање на информациона безбедност (анг. *information security management system - ISMS*). Овој стандард е развиен за да обезбеди модел за воспоставување, имплементација, извршување, мониторинг, ревизија, одржување и подобрување на системот за менаџирање на информационата безбедност. Сертификацијата применува пристап кој се базира на дефинирање на безбедносни политики, дефинирање опфат на системот за менаџирање на информациона безбедност, спроведува проценка на ризик, менаџирање на идентификуваните ризици, определување цели на контрола и подготовка на проценката на применливост.

За споредба, сертификацијата на информациони системи во Република Македонија претставува процес утврден во рамките на Законските и подзаконските акти. Процесот се спроведува согласно Законот за електронско управување и се однесува на институции на кои согласно закон им е доверено да вршат јавни овластувања, односно извршуваат електронски административни услуги и разменуваат документи и податоци по електронски пат. Овие институции се задолжени да го следат процесот на сертификација на информациони системи, а до овој момент се сертифицирани само четири институции во Република Македонија.

Во овој труд накратко се објаснети процесот на сертифицирање на државните органи согласно Законот за електронско управување, процесот на ISO/IEC 27001 сертификација и *COBIT* методологијата. Понатаму со помош на компаративна анализа се утврдени разликите и сличностите помеѓу овие структурирани пристапи во управување со ИС. Врз основа на оваа анализа може да се утврди дали користењето на два или повеќе организирани пристапи во управување со ИС е возможно и дали организацијата (државниот орган) ќе има придобивки од комбинирање на истите.

Abstract

In the past 30 years the application of modern technologies and new work practices enables increased productivity and better communication in the workplace. In order to improve their service organizations and companies establish information systems. An information system is combination of software, hardware and human resources used in order to process and share desired data in more effective manner. But with the continuous improvement of services we are faced with greater challenges to provide continuous functioning of the services we offer. Security threats and problems associated with them are among the most important challenges

.

In order to successfully deal with the security risks the Republic of Macedonia has adopted a legal framework presented in a set of minimum recommendations. This framework which is mandatory for public authorities is described in the Law on Electronic Governance where it has been replicated in the process for certification of information systems. Besides the certification included in the Law as mandatory for the government institutions, there is also international framework which consists of numerous standards or methodologies such as: ITIL, COBIT, ISO certification and others. COBIT and ISO certification are voluntary and can be applied to all organizations including state authorities. If this kind of certification is applied in the state institutions it should be easy to implement and reconcilable with the legislation of the Republic of Macedonia, basically it should correspond with the standards required under the Law on Electronic Management and its bylaws.

Most organizations implement number of security measures to protect their data. Yet without established a structured information security management system the control may be disorganized, inefficient and specified only for a certain number of cases. ISO / IEC 27000 family of standards provides a set of standards for information security management systems published by the International Organization for Standardization - ISO and the International Electrotechnical Commission - IEC. The COBIT methodology, however, is created by the ISACA (Information Systems Audit and Control Association) and ITGI (eng. IT Governance institute) and aims at providing a set of good international practices for structured and standardized process that applies to all areas, not only for IT. The standards represent a framework of policies and procedures that include legal, physical and technical controls in the management of information risk in the organization.

ISO / IEC 27001 contains recommendations for best practices for information security management, risks and controls in the context of an overall information security management system - ISMS. This standard was developed in order to provide a model for establishing, implementing, executing, monitoring, review, maintenance and improvement of the information

security management system. The certification applies an approach based on definition of security policies, definition of the scope of the information security management system, conducts risk assessments, managing the identified risks, determining control objectives and preparing the assessment of applicability.

For comparison, the certification of information systems in the Republic of Macedonia is a process established under the Laws and bylaws. The process is conducted in compliance with the Law on Electronic Management and refers to institutions that by law are entrusted to perform public authorizations or perform electronic administrative services and share documents and data in electronic manner. These institutions are required to follow the process of certification of information systems, and up to this point there are only four institutions in the country that are certified.

This paper briefly explains the certification process of the state institutions in accordance with the Law on Electronic Governance, the process of ISO / IEC 27001 certification and the COBIT methodology. Furthermore by using comparative analysis the paper presents the differences and similarities between these structured approaches for information system management. Based on this analysis it can be determined whether the use of two or more organized approaches for information system management is possible and whether the organization (state institution) will benefit from a their combination.

1. Вовед

Современото работење е незамисливо без примена на информациско-комуникациските технологии. Информациите претставуваат неопходен ресурс од кој зависи опстанокот и развојот на организацијата. Компаниите и организациите стануваат се поотворени, притоа ги поврзуваат и разменуваат своите информациони ресурси со ресурсите на компаниите/организациите со кои соработуваат односно кои вршат испорака, набавка, со потрошувачите, и со останатите компоненти од процесот на секојдневното работење.

Но брзиот напредок придонесува до појава на бројни безбедносни закани. Најчести закани со кои се соочуваме се компјутерски измами, шпионирање, други видови на компјутерски криминал, ризици од надворешни влијанија како поплави, пожар и слично.

Сè почести се случувањата кога организациите трпат штети кои настануваат од т.н. хакерски напади и оневозможување на услугите. Последното истражување од компанијата за компјутерска безбедност McAffe [1] наведува дека економските штети на глобално ниво настанати од компјутерски криминал во просек надминуваат 400 милијарди долари. Како препораки и заклучоци од истражувањето се дека овие видови на напади и претрпени штети ќе продолжат да се случуваат и во иднина, и дека без разлика во кој облик се чуваат информациите сепак истите мора адекватно да се заштитат. Адекватната заштита вклучува и информирање на сите корисници за концептот и мерките на заштита во организацијата. Заштитата на информациите, пред сè зачувувањето на интегритетот и доверливоста на податоците е од примарна важност.

Безбедноста на податоците претставува збир од мерки за заштита во многу поголем опфат од набавка и користење технички решенија кои нудат современа заштита. Само користење на заштитен ѕид или анти-вирусен софтвер не значи дека податоците се безбедни.

Заради овие причини во поново време компјутерската безбедност се претставува како концепт чија цел е да осигури дека безбедноста на информациите е многу повеќе од примена на современи технички решенија. Постојат неколку методологии, концепти и стандарди кои се дизајнирани за да го подобрат Менаџирањето со информационите технологии и безбедноста во организациите. Целта на организациите и компаниите е со имплементација на овие механизми, да се осигурат дека користењето на информатичката технологија е безбедно и помага во постигнување на посакуваните резултати. И покрај тоа што се достапни голем број на концепти, алатки, методологии и стандарди, кога се применуваат независно најчесто не се доволно широко опсежни за да ги опфатат сите потреби на менаџирање со информационите технологии.

Во овој труд се анализирани *ISO/IEC 27001* [2] стандардот, *COBIT 5* [3] методологијата и сертификацијата на ИС согласно Законот за електронско управување [4]. Исто така прикажани се нивните сличности и разлики преку меѓусебна споредба.

Стандардот претставува документ утврден со консензус и донесен од признато тело, со кој (за заедничка или повеќекратна употреба) се утврдени правила, насоки или карактеристики за активности или нивните резултати, со цел постигнување оптимално ниво на уреденост во дадена област.

Примена на стандардизиран и концептуален пристап најпрвин е прифатен од Велика Британија, која преку своето национално тело за стандардизација (анг. *British Standards Institution – BSI*[1] паралелно на *MKS* стандардите) се определила за развој на стандарди кои ќе ја опфатат оваа област.

Стандардите и методологиите за менаџмент на информационите системи за подобро разбирање може да ги групираме во две области:

- Стандарди за управување со информациони системи
- Стандарди за управување со информациона безбедност

Пример на стандарди за кои главниот фокус е безбедноста во ИТ се серијата од стандарди *ISO/IEC 27000*[2]*, NIST 800*[3]*, SOX*[4] и други. Во популарните стандарди за управување/менаџирање со информациони системи најчесто се вклучуваат *COBIT*, ITIL[5], COSO[6] и други. Може да забележиме дека овие две групи на стандарди не се негираат едни со други,туку напротив со нивно комбинирање тие се дополнуваат.

Да се одбере правилната методологија и стандард за управување со ИС и информациона безбедност која ќе биде во согласност со најдобрите практики од индустријата е дилема, со која секојдневно се соочуваат одговорните лица при планирање на развојот на организацијата. Постојат голем број на добри стандарди и поради тие причини се јавува дилема при избор на правилниот, односно соодветниот, во смисла на тоа што нудат и колку истото ќе се вклопи во постојниот развој на организацијата. Како што веќе спомнавме одреден стандард или методологија не може во целост да ги опфати сите приоритети на организацијата, затоа задача на менаџерите и раководството е да разгледаат поголем опфат на стандарди кои постојат на пазарот со цел да утврдат кој е најадекватен со фокус кон управувањето со ИС и информационата безбедност во сопствената организација. Ова е токму целта на овој труд да се прикаже што сè нудат позначајните и позастапените стандарди и методологии за ИС *COBIT 5* и *ISO/IEC 27001*, истите да ги анализираме и споредиме со стандардизација на информациони системи согласно легислативата во Р.М.

COBIT како една од попознатите методологии за управување со ИС се повеќе ги имплементира и аспектите на безбедност, истото е уочливо во Верзија 4 и Верзија 5 од стандардот. Во референциите од *COBIT 5* методологијата *(*анг. *Framework)* може да се забележи дека истиот ги користи и позитивните практики од *ISO/IEC, 27005:2008.* Сепак иако *COBIT 5* дава солидни насоки за тоа што треба да се имплементира во областа на мерките за ИТ безбедност во целост, не укажува како треба истите да се имплементираат.

---

[1] Историја на BSI институт за стандардизација на Велика Британија http://www.bsigroup.com/en-GB/about-bsi/our-history/

[2] Целосен преглед на стандардите од серијата 27000 https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

[3] Преглед на NIST 800 стандардите[20] http://csrc.nist.gov/publications/PubsSPs.html

[4] Преглед на SOX легислатива [21] http://www.soxlaw.com/

[5] Преглед на ITIL библиотеките http://www.itlibrary.org/

[6] Преглед на COSO рамката [22] http://www.coso.org/guidance.htm

Слично на ова многу од стандардите, методологиите чиј примарен фокус е информациона безбедност не обезбедуваат адекватни насоки и препораки како да се постават безбедносните мерки за да соодветствуваат во поголемата слика на менаџмент со информационите системи и процеси.

Стандардите кои ги дефинира и усвојува Република Македонија согласно Законот за стандардизација [18] имаат ознака МКС и нив ги издава Институтот за Стандардизација на Република Македонија (ИСРМ). Стандардите кои се усвоени на меѓународно ниво имаат ознака *ISO/IEC* како заеднички стандард на Меѓународна организација за стандардизација (анг. *International Organization for Standardization - ISO*) и Меѓународната електротехничка комисија (анг. *International Electrotechnical Commission - IEC*), а ако се усвоени во Европа имаат ознака *EN* (европска норма), и за нив се одговорни *CEN* (анг. *European Committee for Standardization*), *CENELEC* (анг. *European Committee for Electrotechnical Standardization*) и *ETSI* (анг. *European Telecommunications Standards Institute*).

Првите стандарди во областа на ИКТ безбедност се изработени и усвоени во 90-тите години на минатиот век *BS 7799-1* и *BS 7799-2* [5]. Меѓународната организација за стандардизација го прифаќа *BS* стандардот и го изработува првиот *ISO* стандард во 2000 година односно *ISO 17799* [6] Информациска технологија – безбедносни техники и насоки за менаџмент со безбедност на информациите, истиот подоцна се ревидира и преименува во *ISO/IEC 27002[27]*. Следен од листата на стандарди поврзани со компјутерската безбедност е *ISO/IEC 27001* стандардот кој е објавен во октомври 2005 година.

ISO/IEC 27000 фамилијата на стандарди, претставува серија на стандарди кои се значајни за сите организации кои имаат потреба за безбедносен менаџмент на своите податоци. При што Меѓународната организација за стандардизација *ISO,* и меѓународната електротехничка комисија *IEC,* континуирано работат на подобрување на заедничките стандарди посветени на безбедност на информациите.

Во Република Македонија овој стандард за безбедност на информациите е веќе прифатен. Односно институтот за акредитација на Република Македонија[7] го има усвоено овој сертификат под името *МКС EN ISO/IEC 27001*. Институтот ова овластување го добива од Закон за стандардизација.

Покрај телото за акредитација во Република Македонија, надлежноста во регулирање на законските рамки за компјутерската безбедност е доделена на Министерството за информатичко општество и администрација и истата е опфатена во Законот за електронско управување. Законот за електронско управување стапи на сила во август 2009 година, а последното дополнување со кое дополнително се регулира материјата е стапено на сила во април 2011 година.

Како дополнување на законската рамка Република Македонија усвојува соодветни подзаконски акти, со цел да го дооформи и регулира процесот на сертификација на Информациони системи. За таа цел во 2009 година е усвоен „*Правилникот за начинот на сертифицирање на информациските системи кои ги користат органите за*

[7] Институтот за акредитација на Република Македонија [17]
http://www.iarm.gov.mk/index.php?option=com_content&view=article&id=53&Itemid=56&lang=mk

комуникација по електронски пат, како и за формата и содржината на сертификатот за функционалност на информациските системи“, а дополнително во 2010 се издадени и насоките за сертификација како и образецот за барање за сертификација на информациониот систем. Со оваа законска рамка, согласно Член 1 од Законот, се уредува работата на министерствата, другите органи на државната управа, организациите утврдени со закон и други државни органи, судовите, јавните обвинителства и државното правобранителство, правни и други лица на кои со закон им е доверено да вршат јавни овластувања, органите на општините, на градот Скопје и на општините на градот Скопје, при размена на податоци и документи во електронска форма, односно остварување на административни услуги по електронски пат, кога тоа е утврдено со закон.

Но покрај државните институции секоја организација може да ги следи позитивните насоки од законот со цел воспоставување позитивни безбедносни практики во областа на ИКТ.

Со овој магистерски труд се анализира процесот на сертификација на информационите системи во државните институции на РМ, а за пример е обработен и дел од процесот на сертификација во една организација, со цел да се прикаже техничката примена на легислативата во работна организација. Со користење на компаративна анализа врз пет дефинирани области целта е да се спореди процесот на стандардизација на информациони системи во Република Македонија, со *ISO/IEC 27001* стандардот и *COBIT* методологијата, за да се утврдат сличностите и клучните разлики во процесите. Анализата дополнително се спроведува со цел да се утврди во колкава мера Република Македонија во своите законски рамки имплементира позитивни практики од меѓународните стандарди, и какви се придобивките од постојниот процес на сертификација. Од компаративната анализа се извлечени дополнителни предлози кои би го подобриле процесот на стандардизација во согласност со законска рамка во Република Македонија. Како за пример е обработен и дел од процесот на сертификација во организација со цел да се прикаже реална примена и детален приказ на постојниот процес на стандардизација на информациони системи во Република Македонија.

1.1 Претходни истражувања

Комбинирањето и меѓусебното усогласување на повеќе стандарди и законски рамки не е новост во ИКТ индустријата, но истото прераснува во тренд кој сè повеќе се практикува. Дел од организациите ја користат оваа можност за искористување на позитивните придобивки (економски бенефит од промоција, поголема безбедност, усогласеност и дефинирани процедури), а дел бидејќи покрај сертификат се задолжени да следат одредена законска рамка која задолжително мора да ја имплементираат.

Не ретко се случува организациите кои работат на носење стандарди да имаат изработено и насоки со цел да се олесни комбинирањето на повеќе стандарди, методологии и законски рамки. Така на пример една анализа *Implementing an ISO-integrated Management System Using COBIT 5 од Opeyemi Onifade*[37] а објавено од *ISACA (*анг. *Information Systems Audit and Control Association)* се користи како насока за имплементација на *ISO/IEC 27001* во централната банка на Нигерија. Она што е посебно интересно е дека анализата претставува практичен пример на комбинација на стандард и методологија при што како насоки за имплементација се користат принципите *COBIT 5.*. Дополнително, обработено е и основно мапирање на *ISO* побарувањата со *COBIT 5* насоките за имплементација, и како насоки за водење на процесот се споредени четири области.

Како интересна литература која ги проучува претходните верзии на *ISO* и *COBIT е* истражувањето *An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls* од *Razieh Sheikhpour* и *Nasser Modiri[26].* Авторите ни потенцираат дека економскиот раст на компанијата е пропорционален со користењето на ИКТ, која е во голема зависност од ризикот и информационата безбедност. За правилно справување со овој ризик авторите препорачуваат користење и комбинирање на повеќе стандарди и методологии, како и задолжително воведување на систем за менаџирање со информациона безбедност. Истражувањето може да се оцени како позитивно посебно во делот на табеларниот приказ каде процесите од претходната верзија на *COBIT* методологијата се споредуваат со *ISO/IEC 27001* контролите, но во друг дел во кој се тврди дека системот за менаџирање на информациона безбедност мора да го следи Plan do check act Моделот (истото е точно само верзијата на ISO/IEC 27001 : 2005), и не е задолжително за други стандарди и методологии кои имаат дефинирано сопствени кружни модели. Авторите потенцираат дека ISO/IEC стандардот го надополнува COBIT во делот на управување со информациона безбедност.

Посебно внимание како корисна и применлива анализа привлекува *A Comparison of IT Governance and Control Frameworks in Cloud Computing* од *Elana Bailey* и *Jack D. Becke[38].* Во последните години трендот на т.н. *Cloud computing* е сè позастапен и оваа технологија соодветно се применува и во Р. Македонија. Да се овозможи соодветно ниво на ИТ управување, менаџирање и контрола во *cloud computing* е предизвикот кој авторите на труд се обидуваат да го актуелизираат. Во трудот се обработува споредба на неколку постојни стандарди и методологии како: *CobiT, COSO, ITIL, ENIA,* и *ISO 27000*. Авторите обработуваат неколку клучни компоненти (како справување со ризикот, менаџмент, управување) на секој од овие модели и како тие компоненти се отсликуваат во *cloud* околината. Како дополнителна вредност на овој труд би го спомнал моделот кој го

развиле од 6 показатели: **Процес** (што ќе префрлиме на *cloud),* **Испорака** (Како ќе ни биде испорачана *cloud* услугата софтвер, платформа или инфраструктура), **Имплементација** (како ќе се имплементира, **Формирање на *cloud* околина**, **Менаџмент со ризик** (кои се уникатните ризици за *cloud*), **Контроли** (Кои се потребните модификации во постојните контроли од веќе усвоената методологија-стандард). Истите согласно авторите треба да го олеснат мигрирањето кон cloud околината и усогласување со постојните стандарди и рамки. Сепак и самите автори напомнуваат дека областа на управување со cloud околината е во зачеток и не треба во целост да се осврнеме на ова истражување бидејќи со поголемата примена на cloud околината и управувањето со истата ќе се усовршува во иднина.

Потребата за интеграција и комбинирање на законските утврдени рамки во информационите системи на една организација со меѓународните сертификати и методологии не е нешто ново. Ваков модел на истражување успеав да пронајдам изработено уште од 2007 година *Corporate Governance, Internal Control and Compliance - From an Information Security Perspective* од *Christer Magnusson[39]*. Во основа авторот за пореален приказ ни креира една замислена водечка компанија со седиште во САД и ги опишува предизвиците за имплементацијата на анг. *Sarbanes-Oxley Act (SOX)* усвоен 30-ти јули, 2002 со комбинирање на некој од постојните стандарди и методологии. Авторот во својата анализа ги опфаќа следните стандарди и методологии: *COSO-ERM* , *ISO/IEC 20000, ISO/IEC 27000*, *The Security Architecture* и *COBIT.* Притоа како рамка за компарација предлага 11 области: *Audience, Abstraction level, Objective, Internal Environment, Risk Analysis, Control Activities, Monitoring and Improvement, Documentation and Reporting, Budgeting and Return on Investment, External Relationships Incident, Release and Control Management.* Самиот модел на споредба но и трудот во целост е т.н. бизнис ориентиран односно повеќе е земен предвид финансискиот аспект и ризиците за организациите од финансиски аспект. Притоа во заклучоците авторот наведува дека COBIT како методологија е најлесна за имплементација со цел организацијата да ја исполнува законската легислатива односно *Sarbanes-Oxley Act (SOX),* но исто така укажува дека може да го користиме и како рамка за имплементација на другите стандарди.

Трудот *Comparing different information security standards: COBIT v s. ISO 27001*[14] од Varun Arora ни дава поглед во основната споредба на едни од најзастапените компјутерски стандарди истиот ги споредува постарите верзии од стандардите но може да се користи како основа за понатамошни анализи и споредби. Авторот стандардите поврзани со ИКТ ги подредува во две групи и тоа: Стандарди кои повеќе ги опфаќаат безбедносните аспекти на ИТ (анг. Security standards) и стандарди кои повеќе се насочени кон управување со информационите системи. Притоа како најзначајни од двете групи за основна анализа и споредба ги зема *ISO/IEC 27001* и *Cobit 4.1.* Авторот произволно обработува шест области по кои ги мапира (споредува стандардите) и тоа: *Focus (фокус на стандардот), Paradigm (модел), Scope (опфат), Structure (структура), Organizational model (организациски модел), Certification (процес на сертификација).* Целта на трудот е да им се помогне на менаџерите на фирмите и организациите да се одлучат врз основа

на своите потреби каков тип на стандард треба да имплементираат. Од заклучоците авторот потенцира дека и двата обработени стандарди (методологии) имаат предности во одредени области (односно не го опфаќаат во целост менаџирањето со ИКТ), па врз основа на опфатот и потребите на организацијата менаџментот може да одлучи дали да имплементира еден од нив или двата.

Трудот *Comparison of it security standards - 2009* од *Christine Kuligowski[36]* побудува посебен интерес и би го посочил како задолжителна литература. Во трудот се споредува законската регулатива од 2002 во САД (Соединетите Американски Држави) односно законската рамка анг. *Federal Information Security Management Act* со посебен фокус на менаџмент на ризикот и *ISO/IEC 27001* со посебен фокус на менаџирање на информационата безбедност. Историски целосно се опфатени законските рамки кои се од оваа област и кои се задолжителни за националните агенции до 2006 година, и паралелно во воведот е прикажан и хронолошкиот развој на *ISO/IEC 27000.* За разлика од другите трудови во овој карактеристично е што споредбата меѓу законската рамка и *ISO/IEC 27001* не е поделена по области туку се врши мапирање по Процеси и по задолжителната документација, иако понатаму во трудот во Прилозите А и Б е направено и дополнително мапирање по области и специфични контроли. Дополнителна вредност на овој труд е и анализата на ефективноста и примената на законската рамка, имено во истиот содржи статистички податоци на примената на FISMA по области во владините агенции. Овие се преземени официјални статистики, но сепак се значајни бидејќи може да извлечеме одредени заклучоци. На пример по носење на законот во САД само 47 проценти од владините агенции се сертифицирале во 2002, до 2008 тој процент се зголемил на 96 проценти, а министерството за одбрана во САД било најлошо рангирано при проверките иако 40 проценти од системите се наоѓале во истото. За пример во Р.М. Министерството за информатичко општество ги контролира само сертифицираните информациони системи, но не врши и проверки на сите органи за тоа дали треба да се сертифицираат односно на некој начин не ги стимулира да го започнат тој процес.

2. Анализа на процесот на *ISO/IEC 27001* сертификација

Стандардот *ISO/IEC 27001* е дел од серијата стандарди *ISO/IEC 27000,* кои имаат за цел обезбедување достапност, доверливост и интегритет на податоците преку воспоставување механизми за контрола и заштита на истите. Денес кога целото работење во една организација се извршува преку користење ИКТ системи, безбедноста на податоците е навистина важна. Поради постоење на закани од различни извори неопходно е преземање мерки за заштитата од истите. Во денешно време со услови на пазарна конкуренција обезбедување навремена и веродостојна информација претставува услов за успех на една организација. Корисниците имаат потреба од информација која е ажурирана и благовремено доставена.

ISO/IEC 27001 како дел од меѓународната серија на стандарди *ISO/IEC 27000* има цел да овозможи помош на организациите, без разлика на видот или големината, да развијат и применат систем за управување и безбедност за своите податоци, и да се подготват за независно и непристрасно оценување (сертифицирање) на тој систем, што ќе овозможи заштита на податоците како финансиските информации, личните податоци и сл.

Во оваа *ISO/IEC 27000[7]* серија се опфаќаат стандардите кои ги дефинираат побарувањата за Системот за менаџирање на информациона безбедност односно *ISMS* (анг. *Information security management systems*), обезбедуваат поддршка, детаљни упатства и инструкции за целокупниот процес на стандардизација, исто така содржат и специфични секторски упатства за *ISMS* и оценување на усогласеноста со *ISMS*, менаџмент со ризиците и сл. Оваа серија се состои од следниве стандарди кои се меѓусебно поврзани:

- *ISO/IEC 27000* – Систем за менаџирање на информациона безбедност - преглед и речник
- *ISO/IEC 27001* – Информациона технологија – Безбедносни техники – Систем за менаџирање на информациона безбедност – Побарувања. При што последната верзија го подновува стандардот со цел да се рефлектираат измените во технологиите и како организацијата раководи (менаџира) со информацијата.
- *ISO/IEC 27002* – Практика на работење при менаџирање со информационата безбедност.
- *ISO/IEC 27003* – Насоки за имплементација на системот за менаџирање на информациона безбедност *ISO/IEC 27004* – Менаџирање на информациона бе*збедност* - Мерење
- *ISO/IEC 27005* – Менаџирање на ризик за информациона безбедност
- *ISO/IEC 27006* – Побарувања за телата кои овозможуваат ревизија и сертификација на системот за менаџирање на информациона безбедност.
- *ISO/IEC 27007* – Насоки за систем за менаџирање на информациона безбедност (фокусирано на менаџмент системот)

Покрај основните горенаведени стандарди постојат и голем број дополнителни стандарди кои се однесуваат на специфични сектори (области на примена) кои претставуваат еден вид дополнување/објаснување кон *ISO/IEC 27000* серијата на стандардот.

2.1 Стандард *ISO/IEC 27001*

ISO/IEC 27001 е стандард кој е наследен од британскиот стандард *BS 7799* дел 2 објавен во 1999 и ревидиран во 2002 кога како новина во стандардот е применет моделот *PDCA* (анг. *P*lan–*D*o–*C*heck–*A*ct) односно концептот планирај, прави, провери и делувај. Истиот концепт е имплементиран и во *ISO/IEC 27001:2005*. Но со последната ревизија во 2013 стандардот трпи измени меѓу која поважната е и незадолжителната примена на Анекс А и напуштање на концептот *PDCA*.

ISO/IEC 27001 е усвоен како меѓународен стандард во 2005 година, истиот покрај спецификите за системот за менаџирање на информациона безбедност, опфаќа и збир на активности за менаџирање на безбедносниот ризик. *ISMS* претставува сеопфатна рамка за менаџмент која овозможува на организацијата да анализира, идентификува и презема мерки за справување со безбедносните ризици. *ISMS* осигурува дека безбедносните подготовки се добро имплементирани и истите континуирано се обновуваат паралелно со промените настанати од нови безбедносни ризици, ранливости и влијанија врз функционирање на организацијата, што е важна функција во оваа динамична област, истата преставува флексибилен пристап или пристап воден од ризици (анг. *risk driven*).

Стандардот нема ограничување во примената и ги опфаќа сите видови на организации (како компании, државни органи, непрофитни организации), нема ограничување и на обемот на организациите (од мали бизниси до големи интернационални компании), и е прифатлив во сите видови на услуги и индустрии, од што може да заклучиме дека е широко достапен за примена.

ISO/IEC 27001 не ги наложува формално специфичните контроли за безбедност на информации, бидејќи истите варираат и дополнително се специфицираат од организација до организација која го прифаќа стандардот. Безбедносните контроли од *ISO/IEC 27002* се наведени во Анексот А во *ISO/IEC 27001*. Организациите кои го прифаќаат *ISO/IEC 27001 2013* сега имаат избор да изберат кои од наведените безбедносни контроли се применливи во нивните специфични безбедносни ситуации во ИКТ. Покрај веќе наведените контроли за избор од Анекс А, организацијата потенцијално може да одбере и дополнителни опции за контрола. Ова не е случај и кај претходниот *ISO/IEC 27001 2005* стандард во кој контролите од Анекс А беа задолжителни за примена. Важно е да се наведе дека кај *ISO/IEC 27002* пред да се изберат безбедносните контроли потребно е да се изврши целосна оцена на безбедносните информациони ризици што е важен дел од *ISMS*.

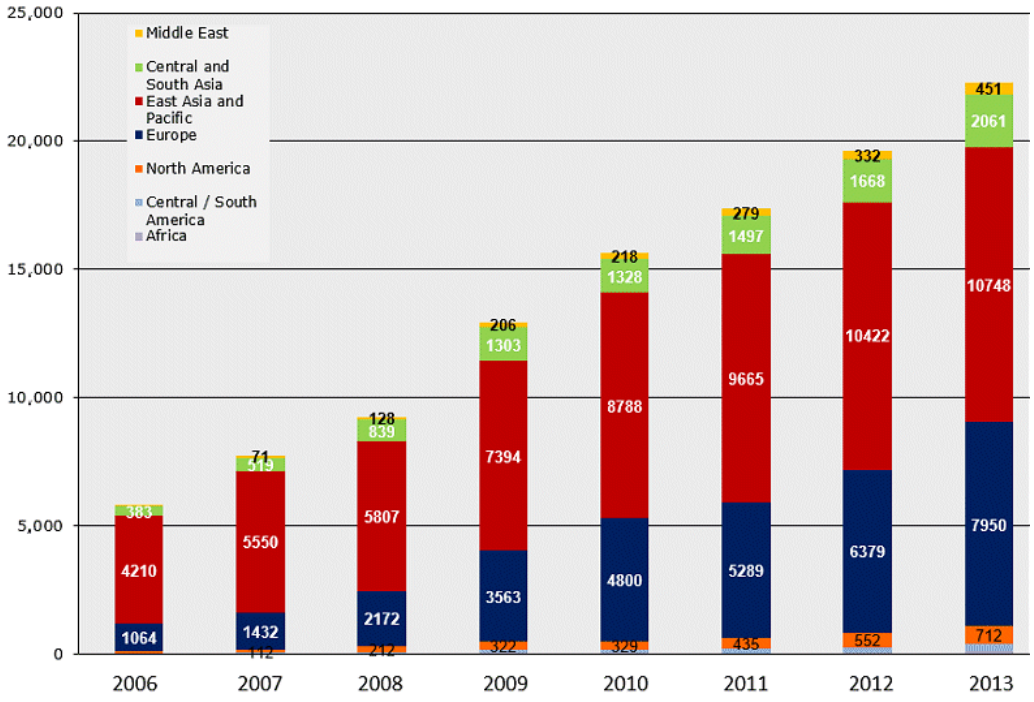
2.2 Структура на стандардот *ISO/IEC 27001*

Стандардот *ISO/IEC 27001:2013* ги содржи следните елементи:

- Запознавање (анг. *introduction*) – Се опишува целта на *ISMS* и како стандардот користи процесен пристап.
- Опфат *(*анг. *Scope)* – Се опишува можноста за имплементација на стандардот во организацијата, поспецифично се дефинираат побарувањата за *ISMS* кои се соодветни за видот и димензијата на организацијата.
- Нормативни референци *(*анг. *Normative References)* – Преглед и речник, во истите се наведува дека само *ISO/IEC 27000* се смета за неопходен стандард за корисниците на 27001, во кој се опфатени прегледот и речникот, останатите следни стандарди од серијата се опциони.
- Поими и дефиниции (анг. *Terms and definitions*) – Краток формализиран речник во кој се вклучени и појаснети основните поими и дефиниции во *ISMS*.
- Контекст на организацијата (анг. *Context of the organization*) – Потребно е за да се специфицираат потребите и очекувањата на организацијата и засегнатите страни, со цел да се специфицира опфатот на *ISMS*. Целта на организацијата е да воспостави, имплементира, одржува и надградува соодветен *ISMS.*
- Раководство *(*анг. *Leadership)* – Се опишува воспоставување на улогата на Менаџментот и раководството кон *ISMS*, раководството мора да демонстрира водство и посветеност кон системот за менаџирање на безбедноста на информациите, да носи политики, и да доделува улоги и одговорности кои се потребни за информациона безбедност.
- Планирање (анг. *Planning)* – Појаснување за воспоставување на стратегиските цели и менаџментот на ризикот во организацијата, се објаснува процесот за идентификација, анализа и планирање за справување со информациони ризици.
- Поддршка (анг. *Support*) – Потребно за да се дефинираат организациските ресурси, познавања, надлежности и потребната документација.
- Работа (анг. *Operation*) – Подетален приказ за проверка и третман со безбедносните ризици, управување со измените, односно безбедносните побарувања на *ISMS* и како да ги третираме истите.
- Евалвација на изведбата (анг. *Performance evaluation)* - Се опишува мерењето на перформансите на *ISMS*, се надгледуваат, мерат, анализираат и дополнуваат безбедносните контроли, процеси и менаџмент системот со цел да се прават системски подобрувања.
- Подобрување (анг. *Improvment*) - Се опишува справувањето со препораките од прегледите и ревизиите, односно нивното континуирано вклучување во надградбата и прочистувањето на *ISMS.*
- Анекс А Референтни контроли и цели за контрола (анг. *Reference control objectives and controls)* - Листа на цели за безбедносна контрола за имплементација на стандардот, подетална листа која соодветствува со делот со контроли во *ISO/IEC 27002.* Овој анекс сега е препорачан за користење не е задолжителен со кој се даваат насоки дека сертифицираните организации би требало да ја користат, но се слободни да ја менуваат и дополнуваат со цел да се специфицира околината во која е воспоставен *ISMS* и специфичните ризици.

2.3 *Сертификација*

Сертификацијата со *ISO/IEC 27001* од страна на акредитирано тело за сертификација не е задолжителна, но истата сè повеќе се бара, како од самата организација, така и од деловните партнери на организациите кои се загрижени за безбедноста на нивните информации, што на некој начин може да се подразбере дека организацијата цели кон воспоставување на систем за безбедност на информациите.
Според истражувањето на *ISO*[8] во 2013 година, имало повеќе од 20.000 ISO/IEC 27001 сертифицирани организации во целиот свет. Податоци прикажани на Слика 1.

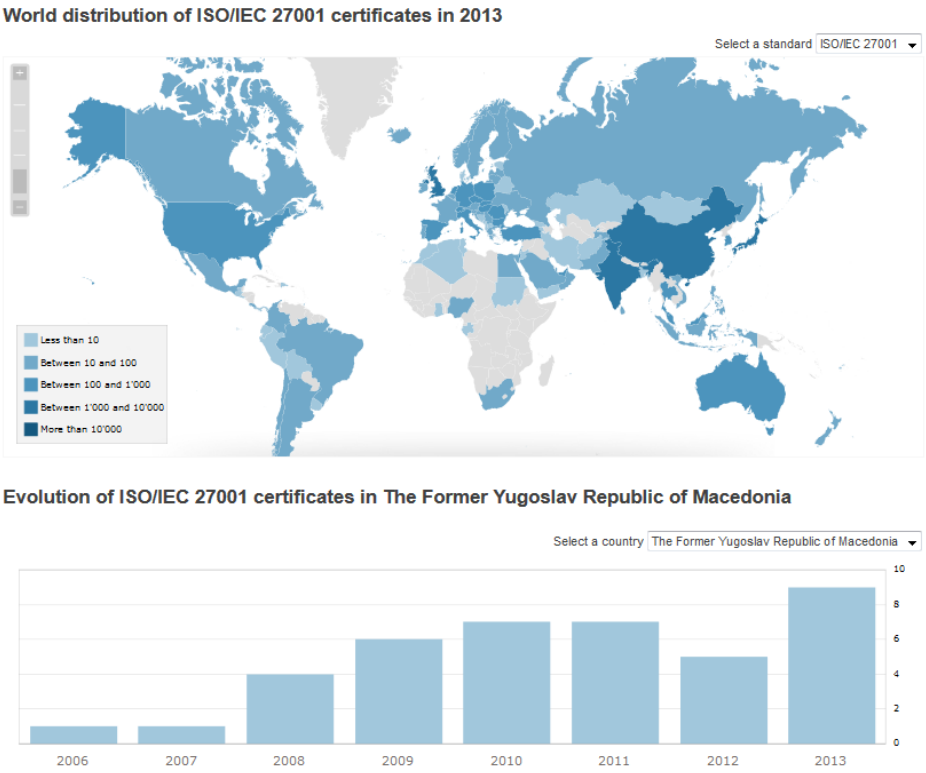


Слика 1 Статистички приказ на вкупниот број на сертифицирани организации

Figure 1 Statistical plot of ISO/IEC 27001 certified companies world wide

Во Република Македонија бројот на сертифицирани организации е на завидно ниво, согласно последно достапните показатели во 2013 бројот на компании кои се сертифицирани е девет податоците се прикажани на слика 2.

[8]Статистички приказ на организации сертифицирани со ISO/IEC 27001 сертификатот
http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC%2027001



Слика 2. Статистички приказ на ISO/IEC 27001 сертифицирани организации во Р.Македонија

Figure 2 Statistical plot of ISO/IEC 27001 certified companies in R.Macedonia

Важно е да се напомне дека на секои 3 години организацијата мора да подлежи и на процес на ре-сертификација, а самиот сертификат не може да трае повеќе од 8 години, ова е рок по кој се објавува излагање на нова верзија од сертификатот. Процесот *на* сертификацијата овозможува многу придобивки: независните ревизии помагаат за поотворен поглед врз процесот на имплементација (значително ја подобруваат информационата безбедност, но и придонесуваат за други придобивки што организацијата ги добива како намалување на ризиците), во имплементацијата побарувањата потребно е одобрување од врвното раководство (што е уште една придобивка земајќи го предвид запознавањето со ризиците и зголемување на свеста). Самиот сертификат дополнително придонесува до зголемување на маркетинг потенцијалот во вид на заложба дека организацијата сериозно го зема предвид менаџирањето со безбедноста на податоците. Она што е важно е дека мора да сфатиме дека самиот сертификат не ја гарантира информационата безбедност на организацијата, со сертифицирање организацијата добива на еден начин независна потврда дека имаат воспоставено соодветен систем за менаџирање со информационата безбедност.

2.4 Задолжителни услови за *ISO* сертификација

ISO/IEC 27001 може да се сфати како формална спецификација за *ISMS* со две различни цели:

- Да се утврди на доста високо ниво, што една организација може да направи со цел да имплементира *ISMS*.

- Опционално по желба може да се користи како основа за формалната процена од акредитирани сертифицирани ревизори, со цел да се сертифицира организацијата. Организацијата е должна да воспостави, имплементира, применува, прати, проверува, одржува и да го подобрува системот *ISMS*, во рамките на сите свои работни активности и ризици со кои се соочува.

Најпрвин е потребно да се дефинира опсегот/опфатот на примена на *ISMS* во односот на организациската структура, локацијата, имотот, технологијата и сл. Она што е важно да запазиме дека сертификацијата се однесува на организацијата, но *ISMS* се однесува на опсегот во којшто е дефиниран. На пример, организацијата може да воспостави опсег на *ISMS* систем во Скопје каде што се наоѓаат и опслужувачите на организацијата, а подрачните единици може и да не бидат опфатени со истиот или делумно опфатени.

Откога ќе се постави опсегот потребно е да се дефинираат цели, правци и принципи односно воопштени политики за безбедност на информациите, притоа мора секогаш да се запазат и надворешните побарувања, законски регулативи договорни обврски со трети страни кои се однесуваат на информационата безбедност.

Во продолжение следи краток опис на целата задолжителна документација која експлицитно се бара за воспоставување на *ISMS* и сертификација:

1. Опсегот на *ISMS* (според клаузулата 4.3)
2. Политика за безбедност на информации (клаузула 5.2)
3. Процесот на оценка на ризик за безбедноста (клаузула 6.1.2)
4. Процесот за третман на безбедноста од ризикот (клаузула 6.1.3)
5. Цели за безбедноста на информациите (клаузула 6.2)
6. Доказ за компетентност на луѓето кои работат во безбедноста на информациите (клаузула 7.2)
7. Други *ISMS* поврзани документи поврзани потребни од страна на организацијата (клаузула 7.5.1b)
8. Оперативни документи за планирање и контрола (клаузула 8.1)
9. Резултатите од оценката на ризикот (клаузула 8.2)
10. Одлуките во врска со третманот на ризик (клаузула 8.3)
11. Доказ за следење и мерење на безбедноста на информациите (клаузула 9.1)
12. *ISMS* програма за внатрешна ревизија и резултатите од извршените ревизии (клаузула 9.2)
13. Доказ за ревизии од врвното раководство на *ISMS* (клаузула 9.3)
14. Доказ за идентификувани несообразености (несоодветности) и преземени корективни мерки кои произлегуваат (клаузула 10.1)
15. Дополнителни други: Анекс А, кој е препорачан, ја споменува но не ја прецизира целосно дополнителната документација вклучувајќи ги и правилата за прифатливо користење на средствата, политика за контрола на пристап, оперативни процедури, договори за

доверливост или не-објавување, принципи за безбедно системско инженерство, процедури за справување со информациони инциденти, релевантна законска рамка, регулации и договорни облигации како и дополнителните процедури за усогласување и процедури за континуирана информациона безбедност. Сертифицираните ревизори речиси сигурно ќе проверат дали овие видови на документација постојат и соодветствуваат со намената. Стандардот не прецизира точно каква форма треба да има документација, но делот 7.5.2 зборува за аспекти како што се наслови, автори, формати, медиуми, ревизија и одобрување, додека контролата 7.5.3 е посветена на контрола на документ, што посочува да се изработи прилично формална што како пример треба да се следи *ISO* 9000.

2.4.1 Опсег на *ISMS*

Стандардот е наменет за да ја води имплементацијата на системот за менаџирање на информациона безбедност (*ISMS*) во рамките на организацијата, притоа осигурувајќи дека сите сектори на организацијата имаат корист од идентификување на ризиците од областа на информатичката безбедност на соодветен и систематски начин. Организациите можат да го приспособат опсегот во нивните системи за менаџирање на информациона безбедност (*ISMS*) согласно сопствените потреби. Определување на опсегот на Системот за менаџирање на информациона безбедност (*ISMS*) е клучна одлука од повисокото раководство во една организација, а документирањето на опсегот на Системот за менаџирање на информациона безбедност (*ISMS*) е еден од задолжителните барања за сертификација.

Иако „Изјавата на применливост“ (*SOA- statement of applicability*) не е експлицитно дефинирана, таа е задолжително барање од точката 6.1.3. Овој термин се однесува на исходот од проценките на ризикот за безбедноста на информациите и особено за одлуките околу справувањето со овие ризици. Изјавата на применливост (SOA) може да биде во форма на матрица на која се прикажани идентификуваните различни видови на информационо безбедносни ризици на една оска, и опциите за справување со ризиците. Таа вообичаено упатува на релевантни контроли од *ISO / IEC 27002*, но организацијата може да се одлучи да користи други рамки како што се *NIST*[8] *SP800-55*[9], на *ISF* стандардот, *BMIS* и / или *COBIT* или сопствен пристап.

Целите на контролата на безбедноста на информациите на ISO / IEC 27002 се дадени во Анекс А, со цел да видливи и да се избегне „неспроведување на потребни контроли“.

Опфатот на Системот за менаџирање на информациона безбедност (*ISMS*) и Изјавата на применливост (SOA) се клучни кога трето лице има намера да определи колку организацијата ги променува начелата на сертификатот *ISO/IEC 27001*. Доколку опсегот на *ISO/IEC 27001* на организацијата се однесува на определен оддел во организацијата во тој случај сертификатот ќе се однесува во врска со состојбата на безбедноста на информациите само и единствено за тој оддел, а не за друг оддел во организацијата или за организацијата во целина. Слично на тоа, за споредба доколку

поради некоја причина менаџментот одлучи да го прифати ризикот од т.н. малвер без спроведување конвенционални анти-вирусни контроли, ревизорите за сертификација може да ја оспорат таквата одлука но, доколку придружните анализи и одлуки биле разумни, ова само по себе не би било оправдување да се одбие да се сертифицира организацијата бидејќи анти-вирусните контроли всушност не се задолжителни.

2.4.2 Процесот на оценка на ризик за безбедноста

Потенцијалните причини за појава на ризици се резултат од внатрешни и надворешни фактори, постојат и специфични ризици кои може да се преклопуваат и во двете области.

Можните последици од појавата на ризикот се:

- незадоволство на клиентите;
- намалување на угледот на организацијата;
- откажување или пропаст на проектираната активност;
- ненадејни и непланирани кадровски измени;
- пречекорување на планираните трошоци;
- временски пречекорувања;
- судски постапки; и др.

Според ***ISO/IEC 27005/31000*****,** управувањето со ризикот претставува плански, активен, структурен, информативен, далекувиден процес кој постојано се развива, менува и постојано се прилагодува паралелно со поставените цели. Потребно е постојано управувањето со ризикот, бидејќи покрај тоа што континуирано се среќаваме со нови ризици, мора и да бидеме внимателни бидејќи може да се променат и постојните, кои исто така, треба да се третираат. Заради тоа важно е да имаме систем на управувањето со ризик кој ќе ги открива и разработува сите ризици, истиот треба да биде дел од сите активности во една организација. При континуираното управување со ризикот се намалуваат несаканите ефекти од потенцијалните ризици.

Работниот опсег на управувањето со ризикот, ги опфаќа ресурсите, интегрираноста на системот, политиките, линиите на комуникација, известување, консултација, разните процеси, алатки и техники со чија помош се обезбедуваат финансиски и организациски ресурси за навремено препознавање, следење, контрола и подобро разбирање на ризиците. Прецизно ги дефинира, овластувањата и одговорностите за ризикот и го одредува нивото до кое треба да се вклучат сите вработени во управувањето со ризикот, во зависност од нивната улога во организацијата. Исто така, обезбедува основа за дефинирање на имплементацијата, мониторингот, контролата, критериумите за оценување на ефикасноста и постојаното подобрување на управувањето со ризикот, низ сите сегменти на организацијата. Овозможува постојана комуникација и со надворешните заинтересирани соработници и обезбедува достапни и сеопфатни известувања за управувањето со ризикот и неговите перформанси.

Со комбинација на веројатностите и последиците од појава/случување на ризичен настан се добива матрицата за анализа на ризик прикажана во Табела1, додека пак оценката дали тој ризик може да го окарактеризираме како прифатлив или неприфатлив е прикажана во Табела2.

Матрица на проценка на ризик			
Веројатност на појава	Тежина на последици		
	Мала	Умерена	Тешка
Не толку веројатно	Ниска (1)	Ниска (2)	Средна (3)
Можно	Ниска (2)	Средна (4)	Висока(6)
Често	Средна (3)	Висока (6)	Многу висока (9)

Табела 1: Матрица на проценка на ризик

Table 1: Risk assessment matrix

Оцена и управување со ризик		
Оцена	Категорија	Објаснување
1, 2	Ниска	Нема потреба од акција, ризикот е прифатлив но потребни се активности за да се осигури дека ќе остане на тоа ниво
3, 4	Средна	Потребни се активности за намалување на нивото на ризик и мораат да бидат планирани. И по реализацијата на активностите потребна е евалвација на ризикот. По потреба се специфицираат и рокови за имплементација на активностите. На Пример до 1 ден.
6, 9	Висока/ Многу Висока	Ризикот е неприфатлив и мораат да бидат преземени акции и мерки за намалување или отстранување. Мораат да бидат преземени превентивни мерки. По потреба се специфицираат и рокови за имплементација на активностите. На Пример до 2 часа.

Табела 2: Матрица за оценување и управување со ризикот

Table 2: Management and assessment matrix

Ризикот претставува ефект од неизвесноста врз исполнувањето на планираните цели и може да биде позитивен или негативен. Според *ISO/IEC 27005/31000* стандардот, ризикот претставува неизвесен настан или состојба, која доколку се појави, има позитивно или негативно влијание на барем една од целите или на главната цел на која било испланирана или проектирана активност во организацијата, на пример, остварување на одредена активност во рамките на договорените трошоци, во договореното време или во договорениот опсег или квалитет. Според тоа, трошокот, времето и квалитетот може да се категоризираат како основни компоненти на ризикот.

Слика 3: Основни компоненти на ризикот

Figure 3: Basic components of risk

2.4.3 Поддршка и проверки на информационата безбедност од страна на врвното раководството

Приоритети на врвното раководство се воспоставувањето на политиките во кои се дефинираат општата определба, насока, или намерата на организацијата. Политиката за безбедност на информации треба да ја изрази посветеноста на менаџментот за имплементација и надградби на сопствениот систем за менаџирање со информациона безбедност *ISMS*, и дополнително треба да ги вклучува целите на информационата безбедност и да обезбедува поддршка во нивниот развој.

Главни задачи на врвното раководство се да обезбеди лидерство кое ќе покаже дека организацијата го подржува *ISMS,* демонстрира посветеност на *ISMS*, се грижи дали *ISMS* полисите и целите се усвоени, води сметка дали побарувањата од *ISMS* станале интегрален дел од процесите во организацијата, води сметка дали се обезбедени потребните ресурси, се грижи дали резултатите од *ISMS* се во рамките на очекувањата. Раководството треба да осигури дека полисите за информациона безбедност се соодветни и во целост ги опфаќаат целите на организацијата.

Дополнително важно е да се доделат одговорности и овластувања за *ISMS,* да се дефинираат безбедносни улоги и одговорности на соодветните лица во организацијата.

Раководството дополнително мора да се грижи за проверките на Системот за менаџирање со информационата безбедност во планирани интервали и тоа најмалку еднаш годишно, со цел да се обезбеди негова континуирана ефективност и подготвеност.

Тие проверки мора да ги опфатат и можностите за подобрувања и промени на *ISMS*, вклучително и политиката за безбедност на информациите и целите за безбедност на податоците. Резултатите од проверките мораат да бидат јасни, документирани и долгорочно архивирани. Притоа потребно е да се дефинираат влезни и излезни елементи на проверките.

Влезните елементи мораат да ги содржат :

- Резултатите од проверките и тестирањата на *ISMS*-от;
- Реакциите и одговорите од вклучените страни (*stakeholders*);
- Процедурите, производите и техниките кои можат да се користат во организацијата за подобрување на перформансите и ефективноста на *ISMS;*
- Статусот на привремените мерки и мерките за корекција;
- Резултатите од мерењата на ефективноста;
- Дополнителните мерки кои се добиени од претходните контроли од страна на раководството;
- Кои било кои измени и влијанија кои можат да влијаат на *ISMS;*
- Препораките за подобрување.

Излезните елементи од проверката мораат да ги содржат сите активности и одлуки кои се однесуваат на *ISMS*:

- Подобрување на ефективноста;
- Обновување на проценатa на ризиците и планот за справување со ризикот;
- По потреба и измените за контролите и процедурите кои имаат влијание на безбедноста на податоците.

2.4.4 Контрола и проверки на системските перформанси

Изданието на стандардот од 2013 бара употреба на метрика на перформансите и ефективноста на Системот за менаџирање на информациона безбедност (*ISMS*) на организацијата и контролата на безбедноста на информациите. Дефинирано во секција 9 „евалвација на перформансите“, побарува организацијата да утврди и да спроведе соодветна безбедносна метрика.

Кога ревидираната верзија од ISO / IEC 27004 ќе биде објавена, истата ќе понуди совети за тоа што и како да мери со цел да се задоволат барањата. Во меѓувреме ISO препорачува примена на пристапот опишан во „PRAGMATIC Security Metrics[9]“

[9] PRAGMATIC Security Metrics: Applying Metametrics to Information Security by W. Krag Brotby (Author), Gary Hinson (Author) [35]

Дополнително внатрешните контроли на *ISMS* мора да се спроведуваат во планирани интервали заради проверка дали целите на контролата, процесите и процедурите на *ISMS.* Истите треба да се:

- усогласени со стандардот, законите и законските акти,
- усогласени со идентификуваните побарувања за безбедност на податоците,
- ефективно имплементирани и одржувани,
- се спроведуваат во рамките на очекувањата.

Овие проверки се водат во рамките на редовна програма, истата се планира земајќи ги во обsир важноста на тековните процеси и областите кои се проверуваа, но и резултатите од претходните проверки. Се дефинираат критериумите за проверките, опфатот на примена, колку често ќе се извршуваат и кои методи ќе се користат. Ревизорите мораат да бидат објективни и непристрасни кон процесот на проверка и не треба да ја ревидираат сопствената евалвација. Одговорноста и условите за планирање и спроведување на проверките, како и евиденцијата и известувањето за резултатите се дефинираат во документирана процедура. Раководството кое е одговорно за областа која се проверува без одлагање треба да преземе мерки за отстранување на неправилностите кои би се утврдиле во текот на проверките.

2.4.5 Континуирано подобрување корективни мерки

Организацијата мора постојано да ја подобрува ефективноста на *ISMS* со користење на политиките за безбедност на податоците, целите за безбедност на податоците, резултатите од проверките, корективните и превентивните мерки и ревизијата од страна на раководството.

Корективните мерки се мерки кои организацијата мора да ги преземе поради отстранување на причините за неусогласеност, како и за да се избегне повторување на неусогласеноста, да се усогласи *ISMS* со постојните промени во ИКТ областа.
Документираната процедура за корективните мерки мора да ги опфаќа побарувањата за :

- Идентификување на неусогласеноста.
- Одредување на причината за неусогласеноста.
- Оценување на потребата од мерки со кои би се осигуриле дека неусогласеностите нема да се повторат.
- Одредување и воспоставување на потребните корективни мерки.
- Евидентирање на резултатите од преземените мерки.
- Преиспитување на преземените корективни мерки.

Превентивните мерки се мерки кои организацијата ги имплементира поради отстранување на причините од потенцијалните неусогласености со цел да се спречи нивното појавување. Преземените мерки мораат да соодветствуваат со потенцијалните проблеми. Документираната процедура за превентивните мерки соодветствуваат како и кај корективните мерки при што мора да ги дефинира барањата за:

- Утврдување на потенцијалната неусогласеност и причината за нејзино појавување.
- Оценување на потребите за мерки со цел да се спречат појавите на неусогласености.
- Одредување и воспоставување на потребните превентивни мерки.
- Евидентирање на резултатите од преземените мерки.
- Преиспитување на преземените превентивни мерки.

Следствено организацијата мора континуирано да ги идентификува и измените на ризиците со цел побарувањата од превентивните мерки континуирано да ги пратат позначајните промени во ризиците. Приоритетите на превентивните мерки се оценуваат врз основа на проценатa на ризиците.

2.5 *Позитивни практики за практична примена*

Позитивни практики кои може да се вклучат во организацијата која се сертифицира:

- Пристапот до личните податоци на организацијата мора да биде ограничен и рестриктивен.
- Во случај на нововработени, при промената на работното место или напуштање на организацијата секогаш се прават корекции на правилата на пристап, нивно надградување, промена или одземање на привилегии.
- Со помош на изјави, правни акти и лични договори треба да се утврдат одговорностите поврзани со безбедноста на податоците.
- Со договорите со трети страни пр. одржување софтверски апликации треба да се вклучат и клаузули за доверливост .
- Во заштитените простории во ниту еден случај не смее да се остават неовластени лица без надзор.
- Кога опремата се остава без надзор треба да се преземат технички или организациски мерки за да се заштитат, пр. за компјутер *Screen Saver* или заклучување на просторијата и сл.
- Обезбедување на редовна заштитна копија (анг. *backup*) на податоците, вклучувајќи ја и документацијата поврзана со имплементацијата од проектите поврзани со ИКТ.
- Целата ИКТ опрема која се отпишува мора да подлежи на процедура за отстранување на информациите кои можат да се содржат на истата на пр. целосно форматирање на диск од принтер или лаптоп.
- Особено внимание и заштита од злонамерни апликации т.н. вируси,тројани и сл.
- Периодични проверки на привилегиите на пристап и периодични промени на лозинките.
- Примена на политики на пр. како „Чисто Биро“, „Чист Екран“ и сл.
- Вработените кои користат преносни уреди надвор од организацијата да потпишат соодветни изјави дека се запознаени со обврските за чување и заштита на податоците.

2.6 *Споредба меѓу ISO/IEC 27001:2005 и 2013*

При анализата и споредбата на податоците од сертификацијата *ISO 27001* и сертификацијата дефинирана во Законот за електронско управување утврдив неколку значајни разлики во самите верзии од стандардот *ISO/IEC 27001* кои се важни да се напомнат. Разликите иако не се премногу сепак се значајни, ни помагаат за да ја согледаме јасната слика од компарацијата помеѓу сертификацијата на ИС согласно Законот за Електронско управување, *ISO/IEC 27001* стандардот и *COBIT* методологијата.

Верзијата од 2013 година е всушност прва ревизија на *ISO/IEC 27001* стандардот и во истата се применети нови концепти, најважно е тоа што во ревидираната верзија се имплементирани практичните искуства од користењето на стандардот.

Дополнително има две позначајни влијанија во ревидираната верзија. Првата е *ISO* побарувањето за нов и ревидиран стандарден менаџмент систем што мора да е во согласност со структурата дефинирана во Анекс *SL*[10] од дел 1 од *ISO/IEC* директивите.

Соодветноста со овие барања треба да придонесат сите стандарди за менаџмент системи да се изедначат, со намера побарувањата од сите менаџмент системи кои не се специфични за одредена област да бидат идентично формулирани во сите стандарди за менаџмент на системи.

Што тоа значи во пракса, сите организации кои имаат воспоставено *ISMS* сега треба да е во согласност со неколку стандарди така на пример *ISO 9001* (стандардот за квалитет), *ISO* 22301 *(*стандардот за бизнис континуитет*)* и се разбира *ISO/IEC 27001.*

Второто позначајно влијание е одлуката да се усогласи *ISO/IEC 27001* со принципите и насоките дадени во *ISO* 31000 *(*менаџмент на ризикот). Ова претставува исто добра вест за интегрираните системи за менаџмент, бидејќи сега организацијата може да ги примени истите мерки и методологии за проценка на ризикот во разни области од работата.

[10] Анекс SL страна 57 од директивата http://www.iec.ch/members_experts/refdocs/iec/isoiecdir-iecsup%7Bed9.0%7Den.pdf

3. Анализа на *COBIT* методологијата

3.1 *Вовед*

*COBIT (*анг. *Control Objectives for Information and Related Technology)* претставува општо применлива и прифатена методологија за добри практики во рамките на сигурноста и управувањето во областа на ИКТ и останатите области поврзани со организациското управување. Истиот е наменет за користење од страна на менаџментот, ИТ корисниците, ревизорите и корисниците кои работат на контрола и безбедност на информационите системи. Стандардот овозможува поддршка во управување со ИТ и обезбедува методи со кои се постигнува усогласеност на ИТ со бизнисот, а со тоа директно овозможува на организациите драстично да ги подобрат работните процеси преку одговорна употреба на ИТ ресурсите и соодветно управување со ИТ ризиците.
Примената на *COBIT* не е условена од ИТ платформата која се користи од организацијата, туку претставува отворен стандард за контрола на информационата технологија. Развиен е и промовиран од *IT Governance Institute.*

COBIT првично бил наменет како помош за :

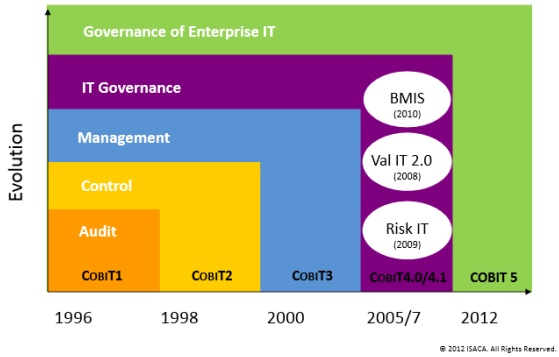
- Менаџерите и раководните лица – на кои им треба да го урамнотежат ризикот и контролата врз непредвидливите опкружувања во ИТ областа.
- Корисниците – на кои им е потребно да добијат осигурување во безбедноста на ИТ услугата од кои зависи испораката на продуктот на организацијата
- Ревизорите – Кои го користат како поткрепа за своето мислење и совети кон менаџментот за ревизијата.

Мисијата на *COBIT методологијата* е да истражува, развива, издава и промовира меѓународен збир на општо прифатени цели за менаџирање со ИТ и други области, во својата рамка ги дефинира следните збирни области/процеси потребни за развој и примена:

- Управување
- Планирање и организација
- Набавка и имплементација
- Испорака и поддршка
- Надзор

За секој од овие области во методологијата се дефинираат т.н. контролни цели и истите се имплементираат со помош на веќе дефинирани потпроцеси. Во публикацијата за *COBIT„"Cobit framework"* [11] се опишани 37 контролни цели-процеси кои спаѓаат во овие пет области. За секој од овие процеси се развиени и обработени детаљни контролни процеси кои вкупно се 318. Понатаму истите дополнително се разработуваат во делот на примена и надзор во публикацијата „*Control Practices*".

[11]Публикација *COBIT framework* http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx



Слика 4: Приказ од најважните промени при историски развој на COBIT превземено од http://www.isaca.org/COBIT/Documents/A-COBIT-5-Overview.pdf

Figure 4: Image of the most significant improvements of COBIT development source http://www.isaca.org/COBIT/Documents/A-COBIT-5-Overview.pdf

3.2 *Структура на COBIT*

Како што беше кажано *COBIT* е креиран од *ISACA (*анг. *Information Systems Audit and Control Association)* и *ITGI (*анг. *IT Governance institute)* и цели кон обезбедување на добри меѓународни практики за темелен, структуриран и стандардизиран процес за управување со ИТ. Со имплементација на *GEIT (*анг. *Governance of Enterprise IT)* и *GTI* (анг. *Governance of IT*) во *COBIT* е воспоставена релација помеѓу ИТ стратегијата и бизнис потребите, се организираат активностите од ИТ прифатените процеси и стандардизирани модели, се идентификуваат клучните ИТ можности и се пренесува влијанието од резултатите во дефинирање на целите на контрола кои се земаат предвид од страна на *GTI*. Мисијата на *COBIT* ги опфаќа областите на истражување, развој, дисеминација и промоција на авторитетот, ажурирање и меѓународното признавање на *GTI* контролите прифатени од страна на организациите, истите сè повеќе се користат од страна на раководствата во бизнисите и од ИТ професионалците.

COBIT гарантира *GTI* (анг. *Governance of IT*) преку структура која ја усогласува ИТ во бизнис стратегија, ја овозможува и поттикнува примената на ИТ во бизнисите и ги максимизира придобивките, осигурува одговорно користење на ИТ ресурсите и соодветен менаџмент во справување со ИТ ризиците. На кратко овозможува соодветно ускладување помеѓу користењето на ИТ и бизнис целите на организацијата.
Структурата на *COBIT* е базирана на две фокус области и тоа управување *(*анг. *governance)* и менаџмент:

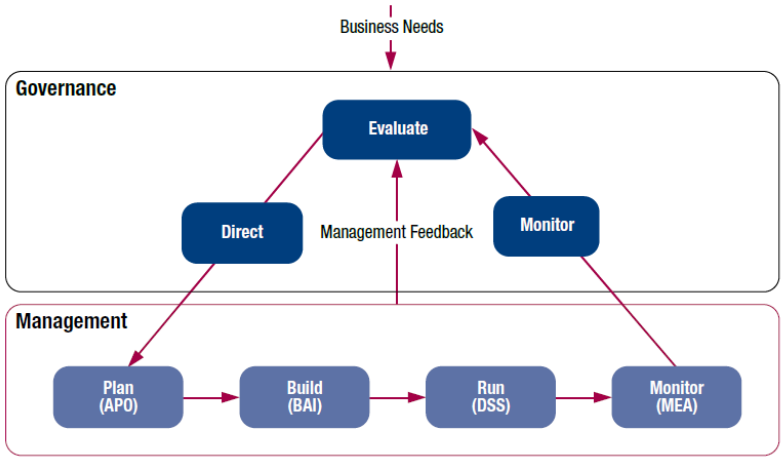
- Управување - се претставува како збир од пет процеси кои се наменети за исполнување на целите на засегнатите страни: вредност на испорака, оптимизација на ризиците и оптимизација на ресурсите, вклучува практики и активности за оценување на стратешките одлуки - Обезбедува насоки за ИТ и ги мониторира резултатите. Врз секој од овие процеси се спроведува методот на проверка *EDM (*анг. ***Evaluate, Direct and Monitor)***
- Менаџмент – Оваа област е опфатена во четири домени:
- Подреди, планирај и организирај *(Align, Plan and Organise)*

- Креирај, набави и имплементирај *(Build, Acquire and Implement)*
- Испорака, услуги и поддршка *(Deliver, Service and Support)*
- Мониторирање, оценување и проценка *(Monitor, Evaluate and Assess)*

За секој од овие четири домени во *COBIT* се дефинирани специфични процеси вкупно 32.

Паралелно на овие две фокусирани области може да увидиме дека во *COBIT* постојат и две различни нивоа на мониторирање. Првиот е важен во контекстот на управувањето т.н. *EDM* модел кој се грижи за транспарентност пред сите вклучени страни и ја појаснува улогата на управата во мониторирање и евалвација на ИТ управувањето, и вториот модел е за менаџирањето и следење на ИТ перформансите кој е генерички за секој од наведените области и служи за воспоставување цели, задачи и нивно мерење прикажани на слика 5.

Во *COBIT* се води сметка за стратешките усогласувања и е посветено големо внимание на поврзување на бизнис планот на компанијата со *GTI*, а со тоа директно се помага во усогласување ИТ со работењето на компанијата. Вредноста на услугите гарантира испорака на целите, ги оптимизира трошоците и ја докажува на вредноста на ИТ во стратешкиот резултат. Управувањето со ресурсите има за цел да се оптимизираат ИТ алатките (апликации, информации, инфраструктура и луѓе), управувањето со критичните ресурси, подобрување на инвестициите и познавањето за овие ресурси.



Слика 5: Поврзаност помеѓу управувањето и менаџирањето во COBIT превземено од http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx

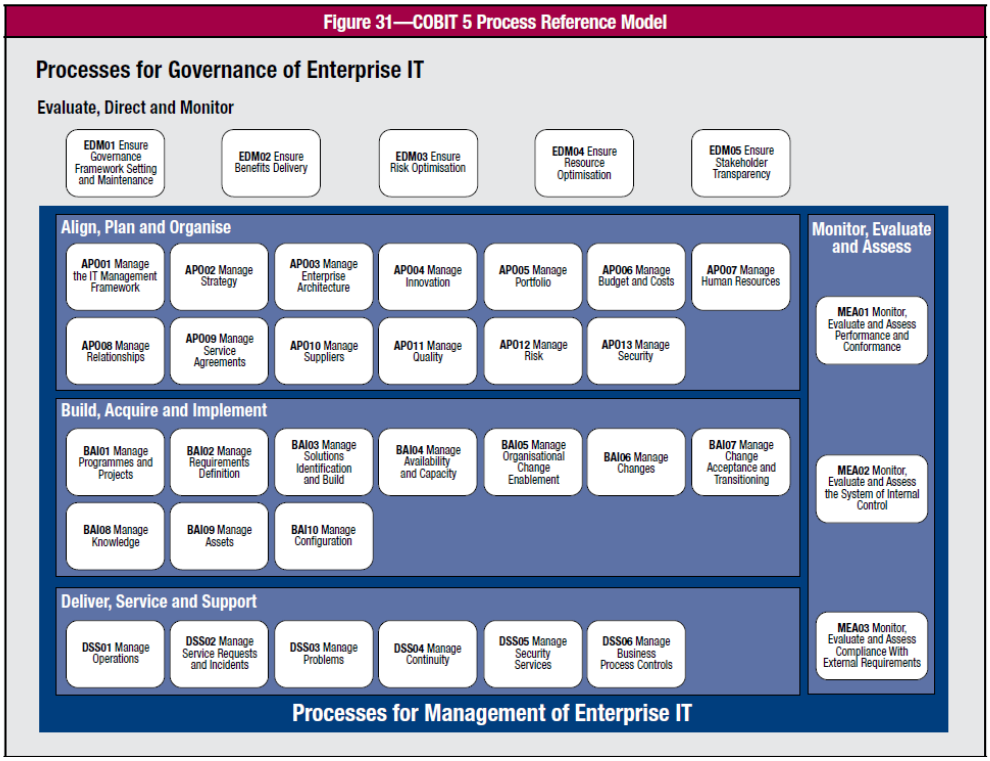
Figure 5: Link between governance and management in COBIT source http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx

Управување со ризикот обезбедува јасна визија на значителните ризици за компанијата, инкорпорирање на одговорностите во управување со ризик на организацијата.
Мерење на ефикасноста го следи спроведувањето на стратегиите, завршување на проектите, како и употребата на ресурсите, изведбата на дадените услуги, балансирање и спроведување на стратегиите во акција за да се постигнат целите.

Притоа *GTI* не треба да се смета само како поддршка за организацијата, туку како основно средство за одржување на административното управување и стратегија на компанијата. Главната цел е да се изгради и одржува поддршката на ИТ алатки. Анализата на овој процес мора да обезбеди и да ја води компанијата во одлучувањето за нови проекти, набавки на нови ИТ алатки и ефикасно искористување на постојните

алатки, следење на технолошките еволуции кои во денешно време се јавуваат доста брзо, често и со радикални промени.

Структурата на *COBIT* е организирана во неколку области, кои се меѓусебно поврзани за да се дефинира модел за процесите поврзани со ИТ. Овие области имаат свои процеси, карактеристики и точни активности. Како што се гледа во *Слика 6*, што претставува целокупната структура на *COBIT,* областите кои вклучуваат планирање и организација, набавки и имплементација, испорака и поддршка и следење и евалвација.



Слика 6 : структура на COBIT превземено од http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx

Figure 6 : Model of the structure of COBIT source http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx

3.3 *Управување*

Во текот на изминатата деценија, поимот „управување (анг. *Governance)*“ сè почесто се интегрира во приоритетите на деловното размислување, овој процес се случува како одговор на позитивните примери кои ја покажуваат важноста на доброто управување. Споредбено на другиот крај на скалата глобалните грешки во бизнисот, односно негативните примери за менаџирање дополнително мотивираат за имплементирање на оваа област во организациите. Успешните претпријатија имаат препознаено дека одборот и директорите треба да ја прифатат ИТ како и секој друга значајна област од водење бизнис. Управувањето и менаџирањето не се спроведуваат одделно едно од друго, туку заеднички при што секоја организација мора самостојно да си ги дизајнира своите планови или насоки, земајќи ги предвид специфичните фактори за организацијата без разлика дали се тоа надворешни или внатрешни.

Одборите и менаџментите во ИТ и бизнис областите, мора да соработуваат и да работат заедно, за да се осигураат дека ИТ е вклучена во пристапот на управувањето и раководењето.

COBIT 5 обезбедува сеопфатна рамка која им помага на претпријатијата во постигнување на нивните цели за управување и менаџирање на ИТ во претпријатието. Едноставно кажано со имплементација на насоките од стандардот директно им се олеснува на претпријатијата да ја искористат оптималната вредност на ИТ, преку одржување рамнотежа помеѓу остварување профит и оптимизација на нивото на ризикот и употреба на ресурси. *COBIT* 5[40] ѝ овозможува на ИТ да биде управувана и менаџирана на сеопфатен начин за целото претпријатие, земајќи ги предвид интересите поврзани со ИТ на внатрешните и надворешни чинители. *COBIT* 5 е генерички и корисен за претпријатија од сите големини, без разлика дали се работи за трговски, непрофитни или од јавниот сектор.

Како што е прикажано на *слика 6* управувањето е интегрирано во целиот стандард, се содржи во сите методологии од самата работна рамка (анг. *framework).*

Карактеристичен е петтиот принцип „*ОДВОЈУВАЊЕ НА УПРАВУВАЊЕТО ОД МЕНАЏМЕНТОТ*“,со кое *COBIT* јасно става на знаење дека во последната верзија се приоритизира областа на управување и јасно ја издвојува од менаџментот. Овие две дисциплини обработуваат различни видови на активности, побаруваат различни организациски структури и служат за различни цели. *COBIT* и ја дефинира разликата помеѓу управување и менаџмент: „Управувањето служи за да обезбеди дека потребите на засегнатите страни, услови и опции се евалвирани за да се одредат балансирани и договорени цели кои треба да бидат постигнати; одредување на насоки преку приоритизирање и носење одлуки; и мониторирање на перформансите и усогласеноста со договорените насоки и цели.“[12] Менаџментот планира, гради и ги мониторира активностите во согласност со насоката одредена од управното тело со цел да се исполнат целите на претпријатието.

Како што спомнавме оваа област служи за да осигури дека целите на организацијата се постигнуваат земајќи ги предвид проценитe од учесниците во бизнис процесот, условите и можностите, поставените насоки кои произлегуваат од приоритетите, правилно донесените одлуки, следење на перформансите на системот, ускладеноста и напредок кон договорените насоки. На кратко во *COBIT* овој термин се дефинира како *EDM (*анг. *Evaluating, Direction, Monitoring*). Процесите кои се опфатени во областа на управување се :

- Осигурување на рамка за управување со подесување и одржување;
- Осигурување на испорака на придобивките;
- Осигурување на оптимизација на ризикот;
- Осигурување на оптимизација на ресурсите;
- Осигурување на транспарентност за вклучените страни.

[12] Принцип 5 страна 14 од*COBIT framework* http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx

3.4 *Менаџмент*

3.4.1 Усогласување планирање и организирање

Процесот на усогласување планирање и организирање на стандардот се занимава со стратегии и тактики. Исто така се фокусира на идентификување на начинот на кој информатичката технологија може најдобро да придонесе за исполнување на бизнис целите. За да се достигне стратешко и визионерско планирање,потребно е заедничко согледување на различните перспективи, дискусии и евалвации. Организацијата што поседува ИТ инфраструктура може да го примени овој модел, којшто најчесто ги опфаќа следните акции :

- Управување со рамката на ИТ менаџмент.
- Менаџирање со ИТ стратегијата.
- Менаџирање со ИТ архитектурата на организацијата.
- Менаџирање со иновациите.
- Менаџирање со портфолиото.
- Менаџирање на буџетите и трошоците.
- Менаџирање на човечките ресурси за ИТ.
- Менаџирање со работните односи.
- Менаџирање со договорите за услуги.
- Менаџирање со снабдувачите.
- Менаџирање со квалитетот.
- Менаџирање со ризиците.
- Менаџирање со безбедноста.

3.4.2 Развој стекнување и имплементација

Развојот стекнувањето и имплементацијата се однесуваат на ИТ стратегијата. Решенијата мора да бидат идентификувани, развиени или набавени, имплементирани и интегрирани во бизнис процесите. Подобрувањата во одржувањето на постојните ИТ решенија се со цел да се обезбедиме дека овие решенија ќе продолжат да ги следат бизнис целите и нормално ќе се справуваат со прашањата побрзани со набавките и имплементацијата. Процесите кои се опфатени во оваа област се :

- Менаџирање со програмите и проектите;
- Менаџирање со дефинирање на побарувањата;
- Менаџирање со решенијата,идентификација и изработка;
- Менаџирање со достапноста и капацитетот;
- Менаџирање и овозможување на организациските промени;
- Менаџирање со промените;
- Менаџирање со промените во прифаќањата и транзициите;
- Менаџирање со знаењето;
- Менаџирање со средствата;
- Менаџирање со конфигурациите.

3.4.3 Испорака, услуга и поддршка

Испорака, услуга и поддршка претставува област во стандардот која ја опфаќа испораката на потребните услуги, вклучувајќи и услуги за дистрибуција,
управување со безбедноста и континуирана поддршка на услугите за корисниците. Оваа област е исто така одговорна за управување со податоци и олеснување во оперативните процеси, вообичаено ги опфаќа и се занимава со следниве прашања на испорака и поддршка :

- Менаџирање со операциите;
- Менаџирање со побарувањата и инцидентите;
- Менаџирање со проблемите;
- Менаџирање со континуитет при испорака услуга и поддршка;
- Менаџирање со безбедносните сервиси;
- Менаџирање со контролите во бизнис процесите.

3.4.4 Мониторирање, оценување и процена

Сите ИТ процеси мора редовно да ги проверуваме со цел да го измериме нивниот квалитет и усогласување со оперативните побарувања. Во стандардот се вклучени и менаџирање со перформансите на активностите и мониторирање на внатрешните контроли, кои всушност се справуваат со следните процеси на мониторирање и евалвација:

- Мониторирање, оценување и процена на перформансите и усогласеноста;
- Мониторирање, оценување и процена на системот за внатрешни контроли;
- Мониторирање, оценување и процена на усогласеноста со надворешните побарувања.

Базирано на овие пет области врз кои *COBIT* е структуриран, методологијата *GTI* дефинира вкупно 37 контролни цели кои треба да се користат за континуиран напредок на овој процес. Овие цели се дефинирани во своите области, ни претставуваат како *GTI* придобива во користењето на структурата на *COBIT*. Податоците на организацијата се генерираат и модифицираат преку ИТ ресурсите, овие податоци се неопходни во областите на планирање и организирање и исполнување на целите. Излезните побарувања од областите на планирањето и организирањето се задолжителни влезни податоци за областите на развој планирање и имплементација како и влезни побарувања за испорака и поддршка. Излезните побарувања од овие домени, пак, се користат како влезни за делот на мониторирање оценување и проценка.

4. Анализа на постојната легислатива и литература за процесот на сертификација на ИС во Р.М.

4.1 Вовед

За развојот на електронските услуги потребно е да има оформено законодавството во кое електронските документи и електронската комуникација се признаваат како правно обврзувачки. Во изминатите години се случуваа чести измени и дополнувања на легислативата во законодавството со цел прифаќање на електронските документи, на пример, за да се овозможи електронско издавање одобрение за градење, во 2013 променет е Законот за градење [10]. Поради овие причини континуирано се оформува и подобрува законската рамка која дополнително придонесува за развој на електронските услуги и податоците да се користат на сигурен начин. Во делот на сертификација на информациони системи како позначајни закони кои се поврзани со процесот може да ги наведеме:

- **Закон за податоци во електронски облик и електронски потпис [11]**

Овој закон одредува специфични детали за електронските пораки, како што е на пример, временска или просторна ознака (печат), идентификатор на системот, издавач на електронски потписи итн. Овој закон и 4 подзаконски акти се усвоени во 2001, но во реалност почна да функционира во 2007 кога е усвоен петтиот подзаконски акт кој уредува кој може да биде издавач на електронски потпис. Моментално постојат два издавачи на електронски потписи КИБС и Македонски Телеком, иако повеќе банки и други институции користат самостојни решенија за свои интерни потреби.

- **Закон за електронско управување**

Со овој закон се регулира начинот на проток на електронски податоци и документи помеѓу министерствата и другите органи на јавната администрација, во однос на реализација на електронски сервиси. Подетаљно, седум подзаконски акти се прифатени за да се овозможи имплементацијата на електронска размена на податоци и електронски документи. Овие подзаконски акти се донесени во јуни 2010 со што подетаљно се опишува: средината за електронска размена, сертификацијата на информационите системи, обликот и содржината за овозможување на административни сервиси и обликот на електронските документи, примена на стандарди и регулативи за електронска комуникација, технички побарувања за електронски сервиси, стандарди и регулативи за информационите системи, како и облик и содржина на администрацијата на базите на податоци.

- **Закон за заштита на личните податоци [12]**

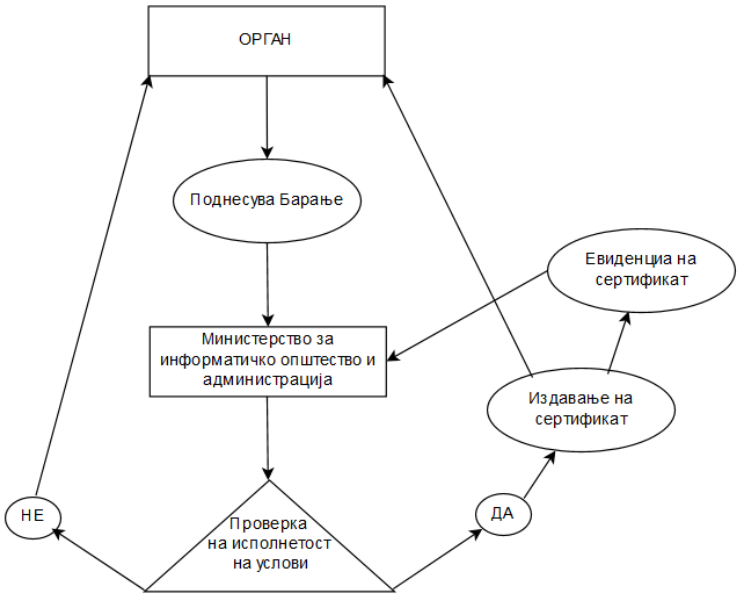
Овој закон се донесе благодарение на потребата за усогласување на легислативата во Р.М. со легислативата во Европската унија. Во законот се опфатени правата и должностите на сите иматели и даватели на лични податоци во Р.М. Со подзаконските

акти во целост е утврден процесот на управување со личните податоци и носење на сите неопходни правилници за управување со личните податоци. Овој закон е важен бидејќи за првпат во делот на ИКТ се специфицираат одговорностите на имателите на личните податоци, што во голема мера значи носење на правилници и специфицирање на процеси за исполнување на услови за обработка на лични податоци.

4.2 Сертификација на ИС во работна организација согласно Законот за електронско управување

Сертификацијата на ИС како законски процес е задолжителна за органите кои вршат размена на документи во електронска форма, односно остваруваат административни услуги по електронски пат. Процесот на сертификација подетаљно е опишана во Правилникот за начинот на сертифицирање на информационите системи кои ги користат органите за комуникација по електронски пат, како и за формата и содржината на сертификатот за функционалноста на информационите системи [13]. Самата сертификација опфаќа неколку законски утврдени процеси и тоа:

- Поднесување на барање за сертификација со придружна документација.
- Процес на проверка на исполнетост на условите.
- Процес на издавање на сертификат.
- Процес на евиденција на сертификатот.



Слика 7 : Дијаграм на процесот на сертификација на ИС согласно закон за електронско управување

Figure 7 : Diagram of the process of certification of IS in accordance with the law on electronic managment

4.3 Процес на поднесување барање за сертификација на ИС

Процесот на барање на сертификација започнува со анализа од страна на органот во однос на тоа за кои од информационите системи кои ги користи за комуникација по електронски пат е потребно да достави барање за сертификација согласно закон до надлежното Министерство за информатичко општество и администрација. Потребно е органот да го утврди опфатот и податоците кои го идентификуваат информациониот систем како и целта на сертифицирањето - приклучување на нов систем на системот за размена на документи и податоци, промена на постоен систем и сл.

При анализата на законската рамка може да се забележи дека „државниот орган доставува барање за сертификација, за секој информационен систем посебно“. Доколку правилно се анализира овој член од Насоките за сертификација на информациони системи, може да се утврди дека овој процес може да опфати повеќе информациони системи во рамките на еден орган.
За споредба може да се разгледаат други типови на сертификација како ISO 27001 и COBIT 5 сертификацијата[14], каде се сертифицира работна организација. Односно со добивање на ваков сертификат се потврдува дека одредена организација го исполнува меѓународниот стандард.

Во легислативата на Република Македонија односно Законот за електронско управување, јасно и недвосмислено се посочува дека се сертифицира информационен систем, односно не се сертифицира органот. Притоа за секој нов систем кој е опфатен со Член 1 од Законот за електронско управување, потребно е органот да достави ново барање за сертификација на ИС, во согласност со Член 4 став 2 од Насоките за сертификација.

Барањето за сертификација се доставува до Министерството за информатичко општество и администрација, притоа секој орган мора да ги пополни предефинираните полиња. Како на пример, назив на органот, седиште на органот, назив на информациониот систем и т.н. Во Табела 1 е прикажано како изгледа едно барање за сертификација.

Земајќи ги предвид моите работни обврски во организацијата во којашто работам како одговорно лице за поддршка на електронски услуги изработив документација која се планира да се достави до Министерството за информатичко општество и администрација, прилог документацијата во овој труд е одобрена за објавување при што чувствителните податоци се отстранети.

БАРАЊЕ ЗА СЕРТИФИКАЦИЈА
на функционалност на информацики систем

Назив на органот:	Заедница на единици на локалната самоуправа на Република Македонија - ЗЕЛС
Седиште на органот:	ул. Копенхагенска бр.5 Скопје
Информациски систем:	„ЗЕЛС – ЕЛЕКТРОНСКИ УСЛУГИ“
Модел:	/
Верзија:	Верзија 1
Опсег на информацискиот систем кој треба да се сертифицира	[*Опис на*: - *инфраструктура* - *хардверски елементи* - *софтверски елементи* - *функционалности (услуги)* - *мрежа* - *човечки ресурси* - *податоци (регистрирани бази на податоци)* - *други елементи релевантни за сертификацијата*]

Табела 3: Барање за сертификација на функционалност на информациски систем

Table 3: Request for certification of the IS functionality according to law for electronic management

Подетаљни информации во однос на опсегот на информациониот систем кој треба да се сертифицира, се прилог бр. 1 на ова Барање.

Како прилог на барањето го доставуваме опсегот на информациониот систем

1. Инфраструктура на информациониот систем

Информациониот систем на ЗЕЛС е составен од голем број на хардверски и софтверски елементи. Системот поседува посебен хардверски sид за превенција од надворешни упади во системот преку кој се спроведени 2 интернет линии од различни интернет провајдери. Интернет линиите се спроведуваат до серверот на кој се наоѓа уште еден уред кој служи за превенција од упади (TMG Server) како и DNS сервер кој служи за именско опслужување на сајтовите кои се хостираат на останатите сервери на информациониот систем на ЗЕЛС. Под овој сервер се наоѓаат 6 апликативни сервери на кои се опслужуваат софтверски апликации за потребите на општините како и уште еден внатрешен DNS сервер кој служи за поврзување на целиот систем во доменска околина. Системот има два сервера поврзани во кластер технологија на кои се наоѓа MS SQL сервер кој ги опслужува сите софтверски апликации на кои им е потребна база на податоци како и еден MySQL Сервер кој служи за база на податоци за апликациите кои не

работат на Windows платформа со соодветна верзија на Apache апликативен сервер. Сите податоци се запишуваат на 2 склада за податоци (storage) кои служат истовремено за чување сигурносни копии со дискови поврзани во различни RAID технологии. Копии од сигурносните копии исто така се чуваат на друга локација надвор од зградата на ЗЕЛС во закупен сеф во банка.

2. Хардверски елементи

- 1 - Firewall Fortigate ----
- 1 - HP ProLiant DL---- 14 GB Ram меморија 1 TB хард диск во раид технологија и два осум јадрени процесори
- 2 - Dell Poweredge R---- 16 GB Ram меморија 1 TB хард диск во раид технологија и два дванаесет јадрени процесори
- 1 - Dell Poweredge R----16 GB Ram меморија 1 TB хард диск во раид технологија и два дванаесет јадрени процесори
- 1 - Dell Powervault ---- 2 TB Поврзани во раид технологија и 1 Hot spare 1 TB диск
- 2 - Storage IBM ---- 20 TB Поврзани во раид технологија и 2 Hot spare 1 TB дискови
- 3 - IBM System ---- 32 GB Ram меморија 1 TB хард диск во раид технологија и два дванаесет јадрени процесори
- 3 - Dell UPS
- 4 - IBM UPS

3. Софтверски елементи

- Апликативните сервери користат Microsoft Windows 2008 R2 додека серверите за бази на податоци користат Microsoft Windows Standard 2008
- FortiOS™
- TMG Server
- DNS
- IIS7, Apache 2.2.17
- SQL cluster, MS SQL Standard 2008, MySQL
- Antivirus eTrust

4. Функционалности (услуги)

- Електронски систем за раководење со градежно земјиште во сопственост на РМ (www.gradezno-zemjiste.mk)
- Софтверско решение за електронско издавање на одобрение за градење (www.gradezna-dozvola.mk)
- Електронски систем за издавање на Б-ИСКЗ дозволи и елаборати (www.ekoloska-dozvola.mk)

5. Мрежа

Надворешната мрежа на системот се состои од 2 интернет линии од различни интернет провајдери спроведени до сервер салата на ЗЕЛС преку оптички кабел до мрежен уред – рутер од каде преку виртуелна мрежа се поврзуваат на информациониот систем во надворешниот хардверски ѕид за превенција од напади (Firewall Fortigate ----)

кој ги спроведува до TMG серверот. Внатрешната мрежа на информациониот систем е составена од 4 мрежни уреди – switch со капацитет 1гигабит на кој се поврзани сите хардверски компоненти на системот во доменска околина и дополнително заштитени од снемување на ел. Енергија со хардверски уреди непрекинато напојување – UPS.

6. Човечки ресурси

Согласно Правилникот за внатрешна организација и систематизација на работните места во стручната служба на ЗЕЛС, утврдена е посебна организациска единица во рамките на ЗЕЛС – Единица за поддршка на е-општини при ЗЕЛС – ЗЕПЕ, која овозможува непрекинат пристап до електронски услуги од домот на административно работење во рамките на делокругот и надлежностите на општините утврдени со Законот, а заради зголемување на ефикасноста, транспарентноста и ефективноста.
Единицата е задолжена за одржување на постојните и развој на нови софтверски решенија, обезбедување и одржување на соодветна хардверска и мрежна опрема и воспоставување и одржување на системот во име на соодветната општина. Организирањето на работите се врши заради намалување на трошоците на општините во доменот на електронските услуги.

Спецификацијата на системот е во согласност со минимално пропишаните технички барања кои се утврдени во друг законски акт - Уредба за минималните технички стандарди и услови во поглед на опремата (хардверот)[13], како и функционалноста на софтверот за електронското јавно наддавање која ја пропишува Министерството за транспорт и врски.

Во уредбата во Член 1 се наведува опфатот на кој се однесува уредбата односно софтверот за електронско јавно надавање на градежно земјиште и се посочува дека со истата се опфатени минималните технички стандарди и услови во поглед на опремата (хардверот), како и функционалноста на софтверот.

Во Член 2 се наведуваат минималните технички спецификации што треба да ги исполнува системот, при дефинирање на истите работната група која ја пишуваше уредбата во која земав активно учество ги зеде предвид и побарувањата на софтверската апликација. Притоа во уредбата се наведува дека апликацијата ќе се води во Заедницата на единиците на локалната самоуправа на РМ и се специфицираат минимални технички стандарди и услови и тоа :

- Најмалку два сервера со минимални карактеристики:
- Четири јадрен процесор со 2 GHz брзина на процесор;
- Четири GB RAM меморија;

[13] Законот за градежно земјиште („Службен весник на Република Македонија“ бр. 17/2011 и 53/2011), Владата на Република Македонија, на седницата одржана на 26.7.2011 година, донесе уредба за минималните технички стандарди и услови во поглед на опремата (хардверот), како и функционалноста на софтверот за електронското јавно наддавање

- Два хард диска од по 120GB (2x120GB) поврзани во RAID технологија;
- Мрежен контролор;
- Оптички уред CD/DVD RW;
- Графичка карта со VGA излез;
- Влезно излезни единици: тастатура, маус, монитор;
- Еден уред за непрекинато напојување со електрична енергија UPS (Unlimited Power Supply) 750 Watt;
- Мрежен уред за поврзување на целиот систем;
- Оперативен систем кој обезбедува работна платформа за функционирање на софтверот за електронско јавно наддавање;
- Централизирано безбедносно решение со антивирус кое обезбедува сигурност на целиот систем од упади, вируси и ја гарантира сигурноста на целиот систем;
- Интернет апликациски сервер кој ги обезбедува сите функции во позадина, а кои се потребни да функционира софтверот за електронско јавно наддавање;
- База на податоци за нормално функционирање на софтверот за електронско јавно наддавање каде што ќе се складираат податоците и ќе се чуваат безбедни;
- Backup решение за базите со податоци;
- Дополнителен надворешен уред за чување на базите со податоци;
- Изнајмена симетрична интернет линија со загарантирана брзина од 2Mbit/s брзина на симнување (download) и 2Mbit/s upload и загарантирана достапност до интернет од 99,99% од времето.

Доколку ги споредиме компонентите барани во уредбата со компонентите со кои располага системот во органот(нашиот случај ЗЕЛС) ќе утврдиме дека во голема мера ја надминуваат минимално законски утврдена спецификација. Притоа мора да наведеме дека во Законот за електронско управување покрај оваа минимална техничка спецификација во условите за сертифицирање точка 3.3.1 од овој труд се побаруваат дополнителни услови кои органот мора да ги исполнува. Како најпроблематични за исполнување би ги напомнал од:

- Точка 1.1 Технички барања во однос на хардверската и софтверската инфраструктура како професионално одржување на константна температура во серверска соба, соодветно електрично напојување, просторните услови (Проект за архитектура доколку постои, се проверуваат просторните услови како дебелина и содржина на sид, метална врата, подлогата под серверите, оддалеченост од водни извори), Физичко обезбедување на просторот и човечки капацитети. Во оваа точка се дефинира минимум две лица потребни за улогите на Мрежен и Системски администратор.
- Точка 1.2 Технички барања кои се однесуваат за размена на податоци и документи како соодветна интернет конекција за опслужување на информационен систем, користење на x.500 сет на стандарди за безбедносните сертификати и директориумските услуги, размена на податоци се врши преку https, за шифрирање на XML се користи *XMLENC.*
- Точка 2.1 побарува уште најмалку две лица и тоа Администратор на база на податоци и ИТ персонал за одржување и поддршка (анг. first level support).

- Точка 4.4 пропишува користење на електронски потпис издаден од владина инфраструктура на јавен клуч, за размена на податоци користење на протоколот *TLS* или *VPN* , поставување на инфраструктура за заштита од напади
- Точка 5.1 побарува дополнителни човечки ресурси за воспоставување на центар за управување со инциденти (Cert тим)
- Точка 5.4 се однесува на обновување по инциденти каде како најкомплициран услов би го спомнал Резервни ресурси на критичните оперативни функции на примарниот систем кои ќе бидат во состојба да ја преземаат функционалноста доколку се случи пад на системот. За исполнување на овој услов односно воспоставена втора локација органот-ЗЕЛС набави услуги на т.н. cloud решение, за во случај на пад на функционалноста за краток период да може системот да биде достапен на друга локација со загуба од податоци не поголема од 15 минути (синхронизацијата на базите на SQL серверот е подесена на тој период).

Органот самостојно одлучува која документација ќе ја приложи, но важно е да се прикаже инфраструктурата, да се опишат хардверските и софтверските елементи, функционалностите (услуги) на системот, да се даде опис на мрежата и документација за човечки ресурси, за да се утврдат капацитетите на органот. Од самото барање може да се утврдат сличности како и кај претходно опишаната *ISO* сертификација, имено кај менаџмент системот за информациона безбедност исто така го специфицираме опсегот. Дополнително карактеристична сличност е и документацијата која се доставува во прилог на барањето за сертификација на И.С. Односно дополнителната документација која се доставува со барањето соодветствува делумно со документацијата која се побарува при *ISO* сертификација. При што може да се заклучи дека истата се користи од различен аспект. Документацијата при *ISO* сертификатот е креирана и обезбедена од самата организација, за истата во позитивните примери и практики од Анекс А содржи и препорака да се креира заштитна (бекап) копија. Документацијата при сертификацијата во рамките на Законот за електронско управување се побарува да се достави како прилог до Министерството за информатичко општество и администрација. Во понатамошната анализа на законската рамка се утврди дека истата се користи при процесот на евидентирање на ИС, односно Министерството за информатичко општество и администрација води регистар на информациони системи и за истите ја чува и обезбедува приложената документацијата. Ова претставува сосема различен пристап споредбено со *ISO* сертификацијата.

По доставување на барањето, следи проверка за соодветност на истото каде се обрнува внимание на формата дали е запазена и дали подносителот може да се идентификува во согласност со законот. Доколку оваа проверка е во ред од страна на Министерството се издава потврда за прием. Последен чекор од процесот на поднесување на барање е проверката на точност на барањето и прилогот доставените податоци. При што согласно Член 27 доколку се утврдат неправилности се дава можност на подносителот истите да ги отстрани.

4.4 Процес на проверка на исполнетост на условите

Процесот на проверка на исполнетост на условите е вториот процес кој може да се извлече од Законската рамка. Законот за електронско управување ја дава можноста за регулирање на овој процес во Член 36 и Член 37. Согласно Законот се укажува на Министерството за информатичко општество и администрација дополнително да го утврди овој процес и се задолжува да врши контрола над функционалноста на информационите системи кои ги користат органите. Овој член од законот ни дава слобода да заклучиме дека Министерството можеме во одредени аспекти да го перципираме и како тело за сертификација споредбено со *ISO*.

Процесот дополнително се регулира во Член 4 од Правилникот за начинот на сертифицирање на информационите системи кои ги користат органите за комуникација по електронски пат, во кој се опишува процесот по прием на барањето и документацијата. Овој процес во правилникот се опишува како утврдување на исполнетост на условите за сертифицирање. Рокот кој се дава на Министерството за утврдување на исполнетост на условите и издавање на сертификатот изнесува 30 дена од денот на прием на барањето.

Дополнително во став 2 од членот се дава можност за утврдување на исполнетост на условите за сертификација да се утврдува и од друго правно лице определено од Министерството. Ова дава простор за слободно толкување дека во иднина може да се очекува зголемување на обемот на сертифицирање на ИС, а следствено и делегирање на надлежноста за проверка на истите на други правни лица. За споредба доколку историски се следи процесот за регистрација на веб страници, кои во минатото ги извршуваше МАРНЕТ во рамките на Министерството сега се извршуваат од приватни компании со овластување. Останува да претпоставуваме дали овој процес на сертификација ќе се придвижи во оваа насока.

Исполнетоста на условите во детали се утврдува во Насоките за сертифицирање. Во насоките се регулираат правата за пристап на лицата кои ја вршат проверките до целосниот систем и потребните документи за системот кој го сертифицираме. За да се овозможи пристап на овие лица законски е специфициран документ „Изјава за заемна доверливост на податоци“ прикажан на Слика 8.

ПРИЛОГ 4

Архивски бр. _____

Дата:

Република Македонија
Министерство за информатичко општество и администрација

ул."Мито Хаџивасилев Јасмин" бр. 50, 1000 Скопје,
Република Македонија
Тел. (02) 3200 870

Факс. (02) 3221 883

Е-пошта: contact_mis@mis.gov.mk
Сајт: www.mioa.gov.mk

ИЗЈАВА

ЗА ВЗАЕМНА ДОВЕРЛИВОСТ НА ПОДАТОЦИ

Сите документи, спецификации, софтвер или податоци за него, оперативни или технички информации, независно дали се дадени во писмена, вербална или електронска форма од било која договорна страна која открива свои доверливи податоци (која понатаму во постапката за сертифицирање ќе се вика „Давател на податоци“) на друга договорна страна (која понатаму во постапката за сертифицирање ќе се вика „Примател на податоци“) во врска со постапката за сертифицирање на информацискиите системи на органот, и кои информации се заштитени на или се сметаат за доверливи од Давателот на податоците и кои, како такви се обележани како доверливи или заштитени или се соопштени во доверба од страна на Давателот на податоците, ќе се сметаат за Доверливи Информации согласно со закон, а нивното користење и чување “Примателот на податоци” ќе го врши врз основа на оваа изјава и согласно со закон.

„Давател на податоци“ „Примател на податоци“

_____ _____

Слика 8 : Изјава за взаемна доверливост на податоци

Figure 8: Statement for mutual data protection-privacy

Во изјавата се потпишуваат овластените лица во име на правните лица, дефинирани како Давател на податоци и Примател на податоци. При што посебно внимание се обрнува на заштитените, тајните и личните податоци. Правната можност за давање и чување на овие податоци е регулирана во Законот за електронско управување во Член 15. Кој вели:

(1) Давателот е должен да собира, да обработува и да дава на користење лични податоци само кога тоа е утврдено со закон.
(2) Личните податоци не можат да се користат за цели, различни од тие што се утврдени со овој закон, освен ако постои согласност на физичкото лице.
(3) Давателот го докажува постоењето на согласност на физичкото лице од ставот (2) на овој член.
(4) Во собирањето, обработката и давањето на користење на лични податоци, давателите се должни да ги применуваат прописите за заштита на личните податоци.

Од што може да заклучиме дека Законот за електронско управување не го уредува само сертифицирањето на информационот систем туку се грижи и е ускладен и со други правни прописи. Во овој случај се работи за усогласување со законот за лични податоци.

За споредба кај *ISO* 27001 сертификацијата се содржи препорака за усогласување со законската регулатива и други договорни обврски, но истата не е стриктно дефинирана и пропишана и варира од условите.

4.4.1 Услови за сертификација

Условите за сертификација се наведени како задолжителни и се опфатени во законската рамка. За дел од условите Министерството побарува и дополнителна документација која се дава на увид при контролата.
Од условите најпрвин се утврдуваат:

1. Техничките барања, начин на работа и функционирање на комуникацискиот клиент.

1.1 Технички барања во однос на хардверската и софтверската инфраструктура на комуникацискиот клиент. Во истите организацијата треба да обезбеди потврди и докази за обезбедување на физичките услови. При што се обрнува посебно внимание на:

- Температурата во серверската соба (Спецификација на клима уредот, дали се работи за професионален клима уред, подесувањето за одржување на температура, гаранција и сервис за одржување);
- Електричното напојување (Проект за електрика, напојување на системот преку различни електрични канали ел.осигурувачи, УПС уреди за непрекинато напојување или дополнителен агрегат и обезбедување услови за негово функционирање во случај на поголем прекин на електрична енергија);
- Просторните услови (Проект за архитектура доколку постои, се проверуваат просторните услови како дебелина и содржина на sид, метална врата, подлога под сервери, оддалеченост од водни извори и сл.);
- Физичко обезбедување на просторот (се проверува дали постои ограничување и контрола до просторот кој се обезбедува само од овластени лица, пристап со картички, видео надзор или држење на просторијата под клуч);
- Назначување на лица (Потребно е да се донесат одлуки од организацијата за назначување на лица кои ќе ја извршуваат работната функција на мрежен администратор и системски администратор). Одлуката треба да ги содржи следните задолженија што треба да ги извршуваат мрежниот и системскиот администратор:

Согласно побарувањето во мојот обработен пример ги дефинирам следните обврски на системскиот администратор, истиот е должен да ги врши следните работи и задачи:

- Врши анализа и проценка на ризиците на информациски систем на ЗЕЛС;
- Врши креирање, имплементација и развој на целокупниот процес на информативна сигурност;

- Врши ревизија на инциденти поврзани со нарушувањата на безбедноста на информацискиот систем во согласност со интерно регулираните процедури за управување со информацискиот систем;

- Го определува нивото на пристап до документите/информациите содржани во информацискиот систем во согласност со законските регулативи со кои е уредено користењето на соодветната апликација;

Мрежниот администратор е должен да ги врши следните работи и задачи:

- Врши доделување на корисничко име и лозинка на именувани/овластени лица во согласност со определеното ниво на пристап до апликацијата во информацскиот систем;

- Се грижи за имплементација на интерните процедури за управување со информацискиот систем.

1.2 Технички барања кои се однесуваат за размена на податоци и документи. За истите организацијата треба да обезбеди потврди и докази:

- Институцијата/органот поседува активна интернет конекција (се доставува доказ од институцијата дека поседува активна интернет конекција, како доказ за јавна набавка, договор за поврзување и сл.);
- Во рамките на органот се користат веб прелистувачи или специфични клиентски апликации кои дозволуваат директен пристап до интернет базирани сервиси, сервери за електронска пошта и други ресурси. (Се опишуваат процедурите доколку постојат за пристап до интернет сервиси);
- Адресите на електронската пошта на јавната и државната администрација е во поддоментите на доменот на влада на Р.М. односно *gov.mk* (Се обезбедуваат докази за регистрација односно сопственост на доменот/поддоменот на институцијата, доказ за воспоставен опслужувач за електронска пошта или сервис за е-пошта);
- Институцијата за обезбедување на административни услуги по електронски пат има можност за размена на пораки по електронска пошта користејќи сметки од службена електронска пошта. (Проверка дали постојат процедури за задолжително користење на службена електронска пошта, дали услугата на системот кој се сертифицира користи сервис за електронска пошта и доколку користи истите се од службена електронска пошта);
- При користење на безбедносни сертификати и директориумски услуги се користи *x.500* сетот од стандарди. (Се проверува дали при користење на административната услуга се користи сертификат во согласност со x.500 сетот од стандарди);
- Проверка на размената на податоци преку протоколите : *HTTP, LDAP, FTP* и други *(*Се проверуваат протоколите кои се користат за размена на податоци, се препорачува користење на *HTTPS);*

- За шифрирање на *XML,* пораките се користи *XMLENC (*проверка дали при користење на *XML* се користи јава библиотеката за енкрипција *XMLENC.*

2. Барања за информатичкиот систем кој поседува електронски регистар.

2.1 Назначување на лица на позициите:

- Администратор за база на податоци и ИТ персонал за додржување и поддршка. Бидејќи оваа точка се однесува на управување со регистар се специфицираат дополнително потребни улоги. Односно потребно е да се донесат одлуки од организацијата за назначување на лица кои ќе ја извршуваат работната функција на администратор на база на податоци и ИТ персонал за одржување и поддршка).

  Одлуката може да биде во следниот формат:

  Одлука лицето ------- вработен во Заедницата на единиците на локалната самоуправа на Република Македонија-ЗЕЛС, на работно место: советник за информатичка технологија, се определува за администратор на базата на податоци во информациониот систем на ЗЕЛС.
  Администраторот на базата на податоци е должен да ги врши следните работи и задачи:

  А) Конфигурирање на базата на податоци;
  Б) Одржување на базата на податоци:
  - Креирање сигурносна копија,
  - Враќање на базата на податоци во претходна состојба во случај на корупција на истата.

  В) Управување со безбедноста на базите на податоци:
  - Менаџирање на најави,
  - Управување со корисници.

  Г) Оптимизација на базата на податоци:
  - Ефикасност на базата (оптимизација на ресурсите и перформансите на базата на податоци),
  - Висока достапност (обезбедување на т.н мироринг, репликација, кластер).

2.2 Воспоставување на процедури за:

- Правење резервни копии (Се проверува дали постои задолжителна пишана документација за креирање на резервна копија (анг. *backup*), се поверува дали редовно се извршува процедурата, дали истата го опфаќа договорениот опфат на пр. податоците, апликацијата, документацијата и сл.) Правилник за правење резервни копии[14].
- Одржување и ажурирање на податоците во регистарот (Се проверува дали постојат процедури и документација за одржување и ажурирање на податоците во регистрите. Доколку органот нема интерни капацитети за одржување и надградби

[14] Прилог 1 од овој магистерски труд

се проверува дали постои договор за одржување. Процесот на пријава и справување со пријави за одржување и ажурирање, на пример време на пријава, одзив по пријава, креирање заштитна копија пред интервенција и сл.).

2.3 Воспоставени се параметри за пребарување на податоците со цел идентификација на поединечни записи (Се проверуваат параметри за пребарување на податоците за идентификување на записите, пр. Архивски број, датум на поднесување или обработка,одговорно лице,статус на предмет и сл.).

2.4 Можност за конверзија на податоците од електронскиот регистар во податоци со *XML* формат (за да се осигури стандардизирана (структура, формат) размена помеѓу два регистра, доколку има потреба треба да постои можноста за конверзија на податоците во *XML.*

3. Барање за оценка и управување на ризикот.

3.1 Органот има воспоставено структуриран пристап во управување со ризиците *(* Се побарува документација план со кој се потврдува воспоставување на структуриран пристап за управување со ризици, се идентификуваат соодветните акции на менаџментот, се дефинираат можните ресурси, одговорности и приоритети за управување со ризиците*)*.

3.2 Процес на управување со ризиците (се објаснува процесот за идентификација, анализа и планирање за справување со информациони ризици.):

- Оценка на големина на ризик
- Избор на ефективни и економски мерки за нивно намалување
- Спроведување на ефективни и економски мерки за нивно намалување
- Оценка дали преостанатите (резидуални) ризици се во прифатливи граници

3.3 Процесот за управување на ризици треба да ги вклучува следните фази:

- Избор на објектите кои ќе бидат предмет на анализа
- Избор на методологија за оценка на ризикот
- Идентификација на информационите средства
- Откривање на слабостите / ранливоста на информациониот систем /средствата
- Анализа на заканите и можните последици од истите
- Оценка на ризиците
- Избор на заштитни мерки
- Реализација и проверка на ефикасноста и ефективноста на избраните мерки
- Оценка на преостанатите (резидуални) ризици

3.4 Органот спроведува проценка и оцена на ризиците по однос на безбедноста на информациониот систем (се проверува дали органот има документација за утврден интервал на проверка и оцена на ризиците, се проверува и методологија за оценка на ризикот).

4. Барања за доверливост на информациите и нивоата на пристап до нив. Министерството во насоките за сертификација ги пропишува нивоата на пристап за доверливост на податоците, при што одредени задолжителни точки се однесуваат само за податоци со поголема доверливост. Дефинирани се следните нивоа на пристап:

- Ниво 0 – Ниво на слободен пристап*;*
- Ниво 1 – Ниво на слободно управување на пристап*;*
- Ниво 2 – Ниво на природно управување на пристап*;*
- Ниво 3 – Ниво на голема безбедност*.*

  Како забелешка, специфицирани се кои задолжителни точки важат за нивоата на пристап, така за ниво 0 задолжително е барањето од точка 4.1, за Ниво 1 задолжително е барањето од точка 4.1 и 4.2, за Ниво 2 Задолжително е барањето од точка 4.1,4.2 и 4.3 и за Ниво 3 задолжителни се барањата од сите точки.

4.1 Информациите се јавни и општо достапни.

4.2 За пристап до информациите се применуваат следниве основни мерки:

- Корисниците се идентификуваат, пред да можат да преземаат каква било акција – автентикација (за утврдување се проверува информациониот систем и техничката документација од истиот);
- За докажување на идентитетот се користи заштитен механизам од типот корисничко име/лозинка, без дополнителни проверки за основните податоци на корисникот (Основно ниво на проверка на идентификација);
- Пристапот до точно определени информации е пропишан на точно определени корисници- авторизација автентикација (за утврдување се проверува информациониот систем и техничката документација од истиот);
- Воспоставена е доверлива комуникација помеѓу корисниците и системот со користење на криптографски протоколи (задолжително е користење на Алгоритами како *RSA* или *SSH*);
- Информациите кои се користат за докажување на идентитетот на корисниците кои пристапуваат во системот се заштитени од неовластен пристап (се прегледува дали постои енкрипција на податоците, и дали информациониот систем на апликациско ниво и на податочно е соодветно програмиран за да оневозможи неовластен пристап);
- Системот за контрола на пристапот функционира самостојно, заштитен од надворешни влијанија и од обиди да се следи текот на неговата работа
- Информациониот систем располага со технички и/или програмски средства, со кои ќе може периодично да се проверува валидноста на системот за контрола на пристапот;
- Заштитените механизми имаат поминато тест, којшто ќе потврди дека корисникот нема можност да ги заобиколи и да добие неовластен пристап до информациите кои тие ги штитат (Најчесто се обезбедува потврда од производителот на информациониот систем, истата се обезбедува за доказ дека производителот ги исполнил минимум од побарувањата за сертификација при изработка на апликацијата).

4.3 За пристап до информациите се применуваат мерките од 4.2 и следните дополнителни мерки:

- Како механизам за проверка на идентитетот на корисниците се користи електронски потпис. (Се прегледува дали при најава, регистрација или извршување на промени од страна на корисниците системот побарува електронски потпис);

- Независно дали е издаден за употреба во локалната инфраструктура на јавен клуч во рамките на конкретниот орган, или е издаден од надворешен доставувач на доверливи услуги;
- При издавање електронски потпис органот дополнително ги проверува основните податоци за корисникот, без да е потребно негово лично присуство. (Се проверува дали постои документација и процедура за издавање на електронски потпис и дали истата е во согласност со насоките);
- Воспоставена е доверлива комуникација помеѓу корисниците и системот преку *VPN* или протоколите *SSL* или *TLS* (Се прегледува каква комуникација е воспоставена помеѓу корисниците и системот, дали истиот користи *SSL*/ *TLS* сертификат и *https*);
- Доверливиот информационен систем обезбедува реализација на принудно управување на пристапот до сите објекти, според претходно строго дефинирани правила на пристап (Се побарува увид во техничката документација од системот);
- Доверливиот информационен систем обезбедува заемна изолација на процесите преку разделување на адресниот простор (Се врши увид во документацијата и во апликацијата да се утврди дали процесите кои ги користи се поделени во адресниот простор, на пример различен предмет има различен идентификатор во адресниот простор).

4.4 За пристап до информациите се применуваат мерките од 4.2 и 4.3 и следните дополнителни мерки:

- Како механизам за идентификација да се користи електронски потпис издаден од владина инфраструктура на јавен клуч;
- При издавање на електронскиот потпис направена е физичка потврда за идентитет на лицето;
- За остварување на заштитена размена на пораки по протоколите *HTTP, LDAP, FTP* и други се користи протоколот *TLS* или решенијата *VPN* за безбедносно криптирање на сесиите. (Се проверува техничката документација од системот, како и документацијата со имплементираните решенија за размена на податоци);
- За криптирање на *XML* базирани пораки на ниво на сесија се користи протоколот *XMLENC* (Се проверува дали во системот за размена на пораки е имплементирана јава библиотеката *XMLENC*);
- Доверливиот информационен систем не дозволува намалување на неговата безбедност како резултат на долготрајни обиди за нејзино нарушување (Се врши увид во заштитата на системот дали е поставена соодветна инфраструктура која ќе изврши соодветна заштита од напади пр. „Denial-of-service *“);*
- Доверливиот информационен систем има механизми за регистрација на обидите за нарушување на неговата безбедност *(*Се врши увид за тоа дали постојат механизми за запишување на податоците односно безвредносните логови и како се конфигурирани).

5. Барање за следење и управување на инциденти поврзани со информациона безбедност:

5.1 Организиран и воспоставен е центар за управување со инциденти поврзани со

информациона безбедност (*CERT* тим), вклучувајќи и развиени формални процедури за следење и управување со безбедносни инциденти (Дали постои формално процедура за именување, односно интерна систематизација за креирање на безбедносен тим. Дали постојат дефинирани процедури за постапување во случај на безбедносен инцидент).

5.2 Процесот за управување со информационо – безбедносни инциденти ги вклучува следните елементи:

- Откривање на инцидентот (Се врши проверка за процесот на редовна и вонредна проверка);
- Единствена точка за пријавување (Во случај на откривање инцидент се проверува до кое одговорно лице се пријавува);
- Евидентирање (Објаснување на процесот за евидентирање инцидент, пр. Извештај, архивирање и сл.);
- Доделување на приоритет на инцидентот и негова класификација. (Преглед на документацијата за приоритизација на инцидентите, доколку се работи за посебен систем за евидентирање и постапување се врши увид во истиот);
- Проценка на настанот/инцидентот и одлуката за начинот на справување со него;
- Обновување и дефинирање на прво ниво за решавање инциденти и услови за пренасочување на друго повисоко ниво. (Се врши преглед дали органот поседува процедури и кадар за т.н. *first level support* и како се постапува во случај да не може да се отстрани инцидентот);
- Верификација и затворање на инцидентот. (Се врши проверка дали инцидентот е решен);
- Идентификација на потребни подобрувања на процедурите за справување со безбедносни инциденти. (Преглед на инцидентот да се утврди дали се можни подобрувања на процедурите за да се минимизира можноста за негово повторување);
- Следење на инциденти и управување со нивниот животен циклус.

5.3 Правила за управување со безбедносни инциденти (подготвени од *CERT* тимот) ги содржат следните елементи. (Се проверува дали процедурите и документацијата по која постапува одговорниот тим ги содржат следните елементи):

- Список на идентификувани важни функции на системот и приоритет за обновување на функционалноста на системот;
- Список на идентификувани ресурси кои се неопходни за исполнување на критично важните функции (на пример, податочен сервер, апликативен сервер, придружен софтвер *IIS Apache,* Интернет пристап и слично);
- Список на можните инциденти со веројатности за нивно појавување, произлегувајќи од оценките на ризикот;
- Разработени стратегии за обновување на функционалноста на системот (Се проверува документацијата за обновување на функционалноста на системот, пример обновување на податоците на втора локација и ставање на употреба во истата и слични процедури);
- Дефинирани мерки за реализација на стратегиите.

5.4 Идентификувани се ресурсите кои е потребно да се резервираат за обновување на функциите на системот – Во ова барање се наведуваат кои ресурси се задолжителни да се имплементирани од органот, притоа како забелешка се наведува дека органите одлучуваат зависно од моменталните потреби за користење на комбинација од овие правила, при што задолжително е правилото утврдено во ставот 2 (центар за обновување по инциденти).

Барањата кои се однесуваат на оваа секција се следни:

- Паралелно запишување или огледална репликација на чуваните податоци. (Се врши проверка на локацијата на која се запишуваат чуваните податоци, дали истата е конфигурирана за да врши паралелно запишување на податоци како на пр. Во *RAID* ниво, и дали за запишаните податоци се врши т.н. огледална репликација *"mirroring"* односно податоците се реплицираат и на друга локација без разлика дали тоа се врши синхроно или асинхроно во кратки временски интервали).
- Формиран центар за обновување по инциденти, во кој се извршува постојано архивско чување на информациите од системот. (Оваа точка е задолжителна при што под центар се подразбира *CERT* тимот кој е задолжен за постојано чување на податоците, заштитните копии, центарот е задолжен да ги примени процедурите за обновување по инциденти).
- Резервни ресурси на критичните оперативни функции на примарниот систем кои ќе бидат во состојба да ја преземаат функционалноста доколку се случи пад на системот. (Се прегледува дали постојат и од каков тип се резервните ресурси, на пример дали постои втора локација, дали се вклучува само при падови на примарната или функционираат паралелно во т.н. *load balancing*, дали истата е на поголема далечина по можност на друга тектонска плоча и сл.).

5.5 Воспоставена е процедура со која при евидентирањето на настаните и инцидентите се создаваат и чуваат најмалку следниве записи:

- Датум и време на случување на настанот;
- Единствен идентификатор на корисник;
- Тип на настанот;
- Резултат на настанот;
- Извор на настанот;
- Список на засегнатите објекти;
- Опис на измените во системот кои произлегуваат од настанот.

Со опишување на условите може да се увиди дека истите во неколку точки нè потсетуваат на Анекс А од *ISO/IEC 27001* односно *ISO/IEC 27002* сертификатот, за споредба во продолжение и табела од листата за проверки за исполнетост на *ISO/IEC 27001 Слика 9*.

ISO 27001-2005 ISMS Requirements	Yes	No	Partial	N.A.
A12.3 **Cryptographic Controls** Objective: Is the confidentiality, authenticity or integrity of information protected by cryptographic means? A12.3.1 Policy on the Use of Cryptographic Controls: Is a policy on the use of cryptographic controls for the protection of information developed and implemented? A12.3.2. Key Mgmt: Is key mgmt in place to support the organisation's use of cryptographic techniques? Remarks (if any):				
A12.4 **Security of System Files** Objective: Are security of system files ensured? A12.4.1 Control of Operational S/w: Are procedures in place to control the installation of s/w on operational systems? A12.4.2 Protection of System Test Data: Are test data selected carefully, protected and controlled? A12.4.3. Access Control To Program Source Code: Is access to program source code restricted? Remarks (if any):				
A12.5 **Security In Development and Support Processes** Objective: Is the security of application system s/w and information maintained?				

Слика 9. Пример од ISO/IEC 27001:2005 листа за проверки

Figure 9: Image of ISO/IEC 27001:2005 check list

4.5 *Проверка на исполнетост на условите Контрола и оценување на процесот на сертификација на ИС - Записник од извршен службен увид*

Во Насоките за сертификација во Прилог 3 е пропишана формата и содржината на записникот од извршен службен увид за сертификација на ИС. Записникот го потпишуваат службено лице од Министерството за информатичко општество и администрација кое ја вршело контролата на исполнетост на условите и Овластеното лице на органот каде е извршен увидот.

Во истиот се наведува органот кој го поднел барањето, архивскиот број. Притоа во формата се испишуваат заклучоците од увидот за утврдување на фактичката состојба на информациониот систем како и неисполнувањето на одредени ставки од условите за сертификација. Во зависност од тоа се Констатира дали се исполнети или не се исполнети условите.

Важно е да се наведе дека е предвиден случај во Законот Член 37, доколку органот изврши промени на информациониот систем или системот престанал да ги исполнува условите утврдени во прописите за електронско управување, надлежноста за да изврши контролата за функционалноста на информационите системи ја има Министерството за информатичко општество и администрација. Во ваков случај на промена согласно Член 5 од правилникот, органот е должен да го извести Министерството во рок од 1 ден од денот на настанатите измени во системот. По добивање на ваква информација од страна на Министерството се врши повторна проверка за да се утврди дали информациониот систем и понатаму ги исполнува условите согласно Законот, и доколку се исполнети се издава нов сертификат. Односно, во ваков случај се повторува целата постапка за проверка на исполнетост на условите, при што само поднесувањето на барањето сега е заменето со достава на информација за промена во системот од страна на органот.

Во случај органот да не ги исполнува условите, Министерството издава решение за престанување на важноста на претходно издадениот сертификат и тоа во рок до 15 дена од денот на приемот на известувањето.

4.6 Процес на издавање на сертификат

Процесот на издавање сертификат може да го перципираме како трет процес во сертификација на ИС согласно Закон за електронско управување. Издавањето на сертификатот се регулира во правилникот за сертифицирање и тоа во Член 6 во кој се дава законска можност за сертифицирање и Член 7 во кој се опишува содржината на сертификатот, за пример во продолжение прикажан на слика 10.

РЕПУБЛИКА МАКЕДОНИЈА
МИНИСТЕРСТВО ЗА ИНФОРМАТИЧКО ОПШТЕСТВО

СЕРТИФИКАТ

за функционалност на информацискиот систем
на _____

за информацискиот систем

_____
_____
_____

врз основа на член 36 став (2) од Законот за електронско управување („Службен весник на Република Македонија" бр.105/09)
и член 5 став 1 од Правилникот за начинот на сертифицирање на информацискиите системи
и за формата и содржината на сертификатот („Службен весник на Република Македонија" бр._____).

Сериски бр. _____ Овластено лице,

Датум на издавање: _____ _____

М.П.

Слика 10: Сертификат за функционалност на информациски систем

Figure 10: Image of the certificate of IS in accordance to law for electronic management in RM

4.7 Процес на евиденција на сертификатот

Процесот на евиденција на сертификатот претставува завршна фаза на процесот на сертификација. Во законот, овој процес правно е регулиран во Член 34 и Член 35, во кои се опишани начините на евиденција на базите на податоци на органите кои комуницираат меѓусебно. Притоа се наведува дека Министерството за информатичко општество и администрација води евиденција на базите на податоци на органите кои меѓусебно комуницираат по електронски пат како посебна електронска база на податоци, заради остварување на функциите утврдени со овој закон. Формата и содржината на евиденцијата наведена во Член 35, како и начинот на нејзиното водење се пропишуваат од Министерот. Истите се регулирани во подзаконските акти. Органите се должни да доставуваат известување до Министерството за информатичко општество и администрација за воспоставување на базата, за нејзиното одржување и чување, како и за промените што се однесуваат на нејзиниот статус, за кои се собира, користи и се чува базата на податоци. Член 35 се однесува само на чување на податоци за услугата која се испорачува по електронски пат и содржи опис на услугата преку определен технички стандард и спецификација

Подетаљно овој процес е регулиран во Член 8 од правилникот за сертификација. При што се наведува дека процесот на евиденција се врши во електронска форма. При евидентирање задолжително е да се внесат следниве податоци: реден број, архивски број и датум на поднесување на барањето за добивање на сертификатот, назив и седиште на органот кој е подносител, број и датум на издадениот сертификат, податоци за идентификување на информациониот систем како модел верзија, опфат на

информациониот систем, вклучувајќи ги документите и податоците во електронска форма и др. Важно е да се забележи дека при евиденција задолжително е да се запишат сите промени што ќе настанат по првичната евиденција, на пример, повторно издавање на сертификатот поради промени и сл.

5. Компарација помеѓу *ISO* 27001,*COBIT* и сертификација на ИС согласно Закон за електронско управување

Користењето на стандарди во ИТ само по себе не може да гарантира 100 процентна безбедност, но истите ни помагаат да воспоставиме еден тип на репер кој ни помага да се осигуриме дека:

- адекватно ниво на безбедност е исполнето,
- со ресурсите правилно и ефикасно се управува,
- воспоставени се најдобрите практики.

Во овој труд се прикажани и анализирани три примери за стандарди во областа на ИТ од што може да забележиме дека иако поседуваат одредени сличности сепак постојат големи разлики меѓу истите. Така *ISO/IEC 27001* стандардот најмногу се користи за да се адресираат прашања поврзани со информациона безбедност, а не толку за проблеми кои се поврзани со Менаџирање со информационите технологии . Земајќи ги предвид овие генерални цели јасно е дека ISO стандардот не коренспондира со *COBIT* методологијата. Сепак постојат голем број на истражувања[15] кои всушност покажуваат дека комбинирање на овие два стандарда придонесува за поопфатен обем при управување со ИТ во организацијата. „Системите како *COBIT* и *ISO/IEC 27001* можат да бидат користени заедно како основа за развој на солиден процес на информациона безбедност“. Дополнително се препорачува поврзување и мапирање на процесите од *COBIT* со контролните цели од *ISO/IEC 27001*.

ISO/IEC 27001 поседува структура што кога ќе биде применета во организацијата на одреден начин ја гарантира безбедноста на информациите на сите нивоа. Од друга страна проблемите како администрирање и менаџмент кои се опфатени во *COBIT* немаат еквивалента структура во *ISO/IEC 27001* ниту во сертифицираниот ИС согласно законот за електронско управување.

ISO/IEC 27001 и Сертифицираниот ИС имаат специфични задачи-карактеристики наменети кон одржување на доверливоста, интегритетот и достапноста на информациите во организацијата.

Друга важна област која треба да ја согледаме е финансискиот аспект, имено *ISO/IEC 27001* и Сертифицираниот ИС не ја опфаќаат областа на финансиските трошоци. Со двата сертификата се третира ризикот и менаџирањето со ризикот, но не се третира ризикот за да се избегнат зголемени трошоци. Во *COBIT* методологијата исклучиво се специфицира дека се цели да се најде баланс помеѓу оптимизација на ризикот и користење на ресурсите.

[15] Научен труд за позитивното влијание при комбинирање на двата стандарда http://www.sersc.org/journals/IJSIA/vol6_no2_2012/2.pdf

COBIT има предност во проценатa-евалвација на критичните фактори за успех, метриката, индикаторите и ревизиите. Од друга страна *ISO/IEC 27001* и Сертифицираниот ИС имаа предност во менаџментот на ИТ и за прашања од ИТ безбедност.

Од досегашниот преглед на дискутираните стандарди за појасно разбирање може табеларно да се прикажат следните сличности и разлики во Табела 4.

	ISO/IEC 27001	***COBIT***	**Сертифицирање Закон Електронско управување**
Дали стандардот опфаќа информациона безбедност	да	да	да
Дали стандардот опфаќа менаџирање со безбедност на ИТ	да	да	делумно
Дали стандардот опфаќа управување и менаџирање со останатите области поврзани со ИТ	не	да	не
Дали стандардот опфаќа вклучување на високо раководство во дефинирање на опфатот	делумно	да	делумно
Дали постои тело кое врши сертифицирање на системот	да	не	да
Дали е задолжително исполнување на сите услови и контроли за стекнување на сертификат	да и делумно	делумно , сертификат за *COBIT* стекнуваат лица кои потоа вршат проверки	да
Дали стандардот е практичен и скалабилен-надградлив	да	да	Не
Цел на стандардот	Воспоставување на систем за менаџирање со информациона безбедност	Планирање и воспоставување на ИТ процеси	Проверка за Исполнување на предефинирани услови за ИТ безбедност
Организациски модел на кој се однесува стандардот	Менаџментот и ИТ одделот	Сите чинители во процесот	Менаџментот и ИТ одделот

Табела 4: Приказ на сличности и разлики помеѓу стандардите

Table 4: Analysis of the similarities and differences of the discussed standards

5.1 Детаљна компарација *помеѓу ISO 27001,* COBIT *и сертификација на ИС согласно Закон за електронско управување*

За потребите на овој труд ќе анализираме пет основни области на стратешко планирање на компјутерската безбедност и тоа: Идентификација, заштита, откривање-детекција, реакција и обновување по инциденти. Истите *ISACA (*анг. *Information Systems Audit and Control Association)* ги третира како први пет приоритетни области [15] од осум кои ги покрива при тренинг и испорака на услуги. Овие области се покриваат како приоритетни и од други тела за стандардизации на пример и Националниот институт за стандардизација и технологија на САД (анг. *NISIT*) во своите насоки за справување со инциденти [32] ги обработува истите области.

5.1.1 Идентификација

Идентификација е област во која го утврдуваме познавањето на организацијата во менаџирањето со: безбедносните ризици, ресурсите, со податоците и др. Согласно препораките на Микрософт Идентификација е прв чекор во процесот на менаџирање со ризик [29]. Во оваа област на Табела 5 ги прикажуваме споредбите на темите:

- Планирање и управување со ресурси;
- Менаџирање на бизнис околина;
- Управување;
- Проценка на ризик;
- Стратегија за управување со ризик;

Планирање и управување со ресурсите: Податоците, човечкиот кадар, уредите, системите и капацитетите што овозможуваат на организацијата да ги постигне бизнис целите се идентификуваат и менаџираат конзистентно и во согласност со нивната важност во спроведување на бизнис целите и стратегијата за ризици на организацијата.	Идентификација и попис на сите ресурси: уреди и системи во организацијата	COBIT 5 BAI09.01, BAI09.02
		ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
		Насоки сертифицирање 4.5
	Идентификација и попис на сите софтверски платформи и апликации во организацијата	COBIT 5 BAI09.01, BAI09.02, BAI09.05
		ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
		Насоки сертифицирање 4.5
	Мапирање на комуникацијата и текот на податоците во организацијата	COBIT 5 DSS05.02
		ISO/IEC 27001:2013 A.13.2.1
		Услови за сертифицирање 1.2.5 1.2.6 1.2.7
	Каталошко подредување на надворешните информациони системи	COBIT 5 APO02.02
		ISO/IEC 27001:2013 A.11.2.6
		Услови за сертифицирање не, се утврдуваат само процедурите и стандардите за размена со надворешни системи.
	Приоритизирање на ресурсите (како хардверот ,	COBIT 5 APO03.03, APO03.04, BAI09.02

	уредите, податоците и софтверот) се приоритизираат врз основа на класификација, критичност, и бизнис вредност.	ISO/IEC 27001:2013 A.8.2.1
		Услови за сертифицирање 5.3.1, 5.3.2
	Воспоставување на улоги и одговорности за компјутерска безбедност, интерно во организацијата и кон соработниците.	COBIT 5 APO01.02, DSS06.03
		ISO/IEC 27001:2013 A.6.1.1
		Услови за сертифицирање 5.1
Менаџирање на бизнис околина - Мисијата , целите, вклучените страни и активностите во организацијата се приоритизираат; Овие информации се користат за да се информираат лицата задолжени за безбедност, кои имаат одговорности, како и одговорните во носење одлуки за менаџирање со ризици.	Улогата на организацијата во надворешната бизнис околина е идентификувана и комуницирана.	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05
		ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2
		Услови за сертифицирање Не
	Улогата на организацијата во поврзувањето со надворешните сектори е идентификувана и презентирана.	COBIT 5 APO02.06, APO03.01
		ISO/IEC 27001:2013 не
		Не, но во законот за електронско управување и под-законските акти се укажува да се специфицираат кои податоци се споделуваат кон надворешните организации.
	Воспоставени се приоритети за мисијата, целите и активностите во организацијата	COBIT 5 APO02.01, APO02.06, APO03.01
		ISO/IEC 27001:2013 не претежно се побарува документација која е поврзана со компјутерска безбедност, не и општата документација
		Услови за сертифицирање не
	Утврдени и воспоставени се критичните функции и факторите за испорака на критичните сервиси	COBIT 5 не
		ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3
		Услови за сертифицирање Да 5.3.1, 5.3.2
	Утврдени и воспоставени се побарувања со	COBIT 5 DSS04.02
		ISO/IEC 27001:2013 A.11.1.4,

	зголемена трајност како поддршка на испорака на критичните сервиси	A.17.1.1, A.17.1.2, A.17.2.1
		Да Услови за сертифицирање 5.4
Управување: Политиките, процедурите и процесите за менаџирање и надгледување на побарувањата (како регулаторните, правните, ризикот, животната средина) се користат за информирање на менаџментот за ризиците од компјутерска безбедност	Воспоставени се полиси во организацијата за информациска безбедност	COBIT 5 APO01.03, EDM01.01, EDM01.02
		ISO/IEC 27001:2013 A.5.1.1
		Да Услови за сертифицирање 3.1, 5.1, 5.3.4, 5.3.5,
	Безбедносните улоги и одговорности се координираат и во согласност со внатрешните организациски улоги и улогите на надворешните соработници	COBIT 5 APO13.12
		ISO/IEC 27001:2013 A.6.1.1, A.7.2.1
		Услови за сертифицирање 1.1.2, 2.2.1
	Менаџирање и примена на правни и регулаторни побарувања поврзани со информациона безбедност, лични податоци и граѓански слободи и обврски.	COBIT 5 MEA03.01, MEA03.04
		ISO/IEC 27001:2013 A.18.1
		Сертификацијата е основана врз можности дефинирани во Закон за електронско управување.
	Процесите за управување и менаџирање со ризици ги опфаќаат и ризиците од информациона безбедност.	COBIT 5 DSS04.02
		ISO делумно во ISO се опфатени исклучиво ризици од информациона безбедност
		Во сертификација опфатена со закон за Е.Управување делумно опфатени исклучиво ризици од информациона безбедност
Проценка на ризик: Организацијата го разбира ризикот од компјутерски криминал врз секојдневните активности	Идентификување и документирање на слабостите на ресурсите	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04
		ISO/IEC 27001:2013 A.12.6.1, A.18.2.3
		Услови за сертифицирање 3
	Собирање на информации за ИКТ закани и ранливости од различни извори	COBIT не
		ISO/IEC 27001:2013 A.6.1.4
		Услови за сертифицирање не
	Идентификување и документирање на внатрешни и надворешни	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04

	закани	ISO/IEC 27001 не
		Услови за сертифицирање не
	Идентификување на потенцијалните влијанија на ризикот врз бизнисот и веројатноста за негово појавување	COBIT 5 DSS04.02
		ISO/IEC 27001 не
		Услови за сертифицирање не
	Можните закани, ранливости, влијанието врз организацијата и веројатноста за нивно појавување се користат за да се одреди ризикот	COBIT 5 APO12.02
		ISO/IEC 27001:2013 A.12.6.1
		Услови за сертифицирање, делумно опфатено во 3.3.4
	Идентификување и приоритизација на одговорите за ризиците	COBIT 5 APO12.05, APO13.02
		ISO/IEC 27001 не
		услови за сертифицирање Не, делумно опфатено во 3.3.7, 3.3.8
Стратегија за управување со ризик	Воспоставување и ускладување на процесите за менаџирање со ризикот со сите вклучени страни	COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02
		ISO/IEC 27001 не
		услови за сертифицирање не
	Јасно е утврдена толеранцијата на организацискиот ризик	COBIT 5 APO12.06
		ISO/IEC 27001 не
		услови за сертифицирање не

Табела 5: Споредба на обработуваните стандарди во областа на идентификација

Table 5: Comparative table of the discussed standards in the area of identification

5.1.2 Заштита - превенција

Заштитата е област која служи за да ни овозможи непрекината испорака на критичните сервиси во организацијата. Всушност овде се воспоставува систем со кој се менаџираат идентификуваните ризици од претходната област. Тука се применуваат темите како контрола на пристап, тренинг на персоналот, безбедност на податоците и ИТ заштита, дефинирање на процеси и процедури, одржување и др. истите се прикажани во споредба со дискутираните стандарди во продолжение на Табела 6.

Контрола на пристап: Пристапот до објектите на организацијата и ресурсите е дозволен за авторизирани	Менаџирање со идентитетот и описот за авторизирани уреди и корисници.	COBIT 5 DSS05.04, DSS06.03
		ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1,

корисници, процеси или уреди, и авторизирани активности и трансакции.		A.9.4.2, A.9.4.3
		Услови за сертифицирање 4.2.1, 4.2.2,
	Менаџирање и заштита на физичкиот пристап до уредите кои содржат важни податоци	COBIT 5 DSS01.04, DSS05.05
		ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3
		услови за сертифицирање Да, делумно до уредот кој го содржи системот кој се сертифицира 1.1.4
	Менаџирање со т.н. Далечински "remote" пристап	COBIT 5 APO13.01, DSS01.04, DSS05.03
		ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1
		Услови за сертифицирање 4.3.4
	Менаџирање со улогите и дозволите за пристап, пременувајќи ги начелата за најмалку возможни привилегии	COBIT 5 не
		ISO/IEC 27001:2013 A.9.2.3, A.9.4.1, A.9.4.4
		Делумно да кај услови за сертифицирање 4.1, 4.2, 4.3, 4.4
	Заштита на мрежен интегритет, применувајќи мрежна поделба-сегрегација за потребните подмрежи	COBIT 5 не
		ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1
		услови за сертифицирање не
Информирање, тренинг и запознавање на обврски: На вработените, надворешните соработници, партнерите им е овозможено запознавање и едукација за компјутерска безбедност, со цел да се зголеми свесноста и адекватно да ги извршуваат сопствените задачи и улоги поврзани со компјутерската безбедност и полисите и процедурите поврзани со истата.	Тренинг и информирање на сите корисници	COBIT 5 APO07.03, BAI05.07
		ISO/IEC 27001:2013 A.7.2.2
		услови за сертифицирање не
	Информирање за улогите и одговорностите на привилегираните корисници.	COBIT 5 APO07.02, DSS06.03
		ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
		Услови за сертифицирање делумно да 4.1, 4.2, 4.3, 4.4
	Информирање за улогите и одговорностите во системот за надворешните корисници (соработници, партнери и сл.)	COBIT 5 APO07.03, APO10.04, APO10.05
		ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
		Услови за сертифицирање не
	Информирање за улогите и одговорностите во системот за Извршните	COBIT 5 APO07.03
		ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,

	раководни корисници	Услови за сертифицирање не
	Информирање за улогите и одговорностите на персоналот кој се грижи за физичката и информационата безбедност.	COBIT 5 APO07.03
		ISO/IEC 27001:2013 A.6.1.1, A.7.2.2,
		Услови за сертифицирање 2.1.1, 2.1.2 , 1.2.1, 1.2.2
Безбедност на податоци: Информациите и податоците се менаџирани во согласност со стратегијата за ризик, а со цел да се заштити доверливоста, интегритетот, и достапноста на информациите.	Заштита на податоци во мирување	COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06
		ISO/IEC 27001:2013 A.8.2.3
		Услови за сертифицирање 1.1.4
	Заштита на податоци при пренос	COBIT 5 APO01.06, DSS06.06
		ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
		Услови за сертифицирање 4.4.3
	При вадење, трансфер и уништување се извршува формално управување со уредите кои содржат податоци	COBIT 5 BAI09.03
		ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7
		Услови за сертифицирање не
	Обезбедување на соодветен капацитет на системите со цел осигурување на достапноста	COBIT 5 APO13.01
		ISO/IEC 27001:2013 A.12.3.1
		Услови за сертифицирање 5.4.1 , 5.4.2, 5.4.3
	Имплементирање на заштита од несакан проток на податоци	COBIT 5 APO01.06
		ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
		Услови за сертифицирање 4.3.4, 4.3.5, 4.4.3, 4.4.4, 4.4.5
	Имплементирање на механизми за проверка на интегритетот на информациите и софтверските апликации	ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
		COBIT 5 не
		Услови за сертифицирање не
	Имплементирање на	COBIT 5 BAI07.04

	посебна околина за тестирање и развој	ISO/IEC 27001:2013 A.12.1.4
		Услови за сертифицирање не
Процеси и процедури за информациона безбедност: Безбедносни политики, процеси и процедури се воспоставуваат и користат за менаџирање со безбедноста на информационите системи и ресурсите	Креирање на основна конфигурација на ИКТ системи за контрола.	COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05
		ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
		Услови за сертифицирање не
	Имплементиран е т.н. Животен циклус за системски развој со цел менаџирање на системите	COBIT 5 APO13.01
		ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
		Услови за сертифицирање не
	Воспоставени се контролни процеси за промена на конфигурациите	COBIT 5 BAI06.01, BAI01.06
		ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
		Услови за сертифицирање не
	Заштитните копии на информациите се креираат, одржуваат и периодично се тестираат.	COBIT 5 APO13.01
		ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3
		Услови за сертифицирање 2.2.1, 5.4.2
	Воспоставени се политики за регулација на физичката оперативна околина на уредите.	COBIT 5 DSS01.04, DSS05.05
		ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
		Услови за сертифицирање 1.1
	Дефинирана е политика за уништување податоци.	COBIT 5 BAI09.03
		ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
		Услови за сертифицирање не
	Процесите и процедурите за заштита постојано се подобруваат.	COBIT 5 APO11.06, DSS04.05
		ISO/IEC 27001:2013 не
		Услови за сертифицирање 5.2.8
	Воспоставени се планови за Одговор по инциденти, бизнис стабилност, Обновување по инциденти и обновување по т.н.	COBIT 5 DSS04.03
		ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2
		Услови за сертифицирање 5.2, 5.3, 5.4

	катастрофи.	
	Плановите за одговор и обновување по инциденти се тестираат	ISO/IEC 27001:2013 A.17.1.3
		COBIT 5 не
		Услови за сертифицирање не
	Компјутерската безбедност е вклучена во позитивните практики на одделението за човечки ресурси.	COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
		ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4
		Услови за сертифицирање не
Одржување: Одржувањето и поправките на информационите системи и компонентите се извршува во согласност со дефинираните политики и процедури	Одржувањето и поправките на ресурсите и уредите се извршува и евидентира навремено, согласно претходно дефинирани контролни алатки.	COBIT 5 BAI09.03
		ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5
		Услови за сертифицирање 5.2.3, 5.5
	Одржување со пристап преку далечина на уредите е одобрено, нагледувано и се извршува на начин што не дозволува пристап кој не е авторизиран.	COBIT 5 DSS05.04
		ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1
		Услови за сертифицирање не
Користење на заштитни механизми: Воспоставени се технолошки решенија за безбедност кои се менаџираат за да се осигури дека безбедноста и издржливоста на системите и уредите се во согласност со усвоените политики, процедури и договори.	Прегледувањето и увидот во логовите и податоците се извршува и документира согласно политиките.	COBIT 5 APO11.04
		ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
		Услови за сертифицирање Не
	Воспоставена е политика за заштита и ограничување на пристап за преносните уреди.	COBIT 5 DSS05.02, APO13.01
		ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
		Услови за сертифицирање не
	Ограничување и контрола на пристап до системите и уредите, применувајќи го принципот на што помалку дозволени функционалности.	COBIT 5 DSS05.02
		ISO/IEC 27001:2013 A.9.1.2
		Услови за сертифицирање 4.1, 4.2, 4.3, 4.4
	Имплементирана е заштита на компјутерските мрежи во организацијата.	COBIT 5 DSS05.02, APO13.01
		ISO/IEC 27001:2013 A.13.1.1, A.13.2.1
		Услови за сертифицирање не

Табела 6: Споредба на обработуваните стандарди во областа на заштита

Table 6: Comparative table of the discussed standards in the area of protection

5.1.3 Откривање - Детекција

Со примена на процесот на детекција во работната организација сакаме да постигнеме брзо и ефективно откривање на ИТ безбедносни настани. Оваа област е фокусирана на откривање настани, аномалии, безбедност и континуиран процес на откривање и мониторирање. Постојат многу истражувања за процесот на детекција [30] но кај сите може да извлечеме општо прифатен заклучок, а тоа е дека процесот на детекција всушност признава и претпоставува дека несакано дејство се случило во нашиот систем, на пример неовластено лице добило пристап до податоци. Овој процес всушност служи за брзо и непречено да информираме дека нешто несакано се случило и да реагираме на најсоодветен можен начин. Во Табела 7 се наведени позначајни теми во областа на детекција и истите се споредуваат со нивната застапеност во дискутираните стандарди.

Континуирано следење на безбедноста: Информационите системи и уредите се мониторираат на одредени интервали со цел да се идентификуваат потенцијални ИКТ ризици и да се провери ефективноста на воспоставените заштитни мерки	Мрежата се надгледува за детектирање на потенцијални безбедносни закани	COBIT 5 DSS05.07
		ISO/IEC 27001:2013 не
		Услови за сертифицирање не
	Активностите на корисниците се надгледуваат со цел детектирање на потенцијални безбедносни закани	COBIT 5 не
		ISO/IEC 27001:2013 A.12.4.1
		Услови за сертифицирање не
	Детектирање на малициозен код	COBIT 5 DSS05.01
		ISO/IEC 27001:2013 A.12.2.1
		Услови за сертифицирање 4.4.6
	Воспоставено е мониторирање врз користење на надворешните сервиси со цел детектирање на потенцијални безбедносни ризици.	COBIT 5 APO07.06
		ISO/IEC 27001:2013 A.14.2.7, A.15.2.1
		Услови за сертифицирање не
	Се користат редовни скенирања за компјутерски ранливости (Vulnerability scan)	COBIT 5 BAI03.10
		ISO/IEC 27001:2013 A.12.6.1
		Услови за сертифицирање не
Процеси на откривање детекција:	Дефинирање на улогите и одговорностите за	COBIT 5 DSS05.01
		ISO/IEC 27001:2013 A.6.1.1

Процесите и процедурите за детекција се одржуваат и тестираат за да се осигури навремена и адекватна реакција по неочекувани настани	откривање на ризици	Услови за сертифицирање 3.1, 5.1
	Тестирање на процесите за откривање-детекција	COBIT 5 APO13.02
		ISO/IEC 27001:2013 A.14.2.8
		Услови за сертифицирање не
	Информациите поврзани со настани на детекција се комуницираат до соодветните страни	COBIT 5 APO12.06
		ISO/IEC 27001:2013 A.16.1.2
		Услови за сертифицирање 2.1.1, 2.1.2, 3.1, 5.1
	Континуирано подобрување на процесите за детекција	COBIT 5 APO11.06, DSS04.05
		ISO/IEC 27001:2013 A.16.1.6
		Услови за сертифицирање 5.2.8

Табела 7: Споредба на обработуваните стандарди во областа на откривање-детекција

Table 7: Comparative table of the discussed standards in the area of detection

5.1.4 Реакција

Реакција е област во која ги утврдуваме насоките, полисите и процесите што ќе ни овозможат да реагираме професионално и ефикасно по настанат инцидент, со што индиректно ќе ја ограничиме настанатата штета и нејзиното проширување. Многу организации го учат ова на потешкиот начин, односно на некој начин се чека и игнорира воспоставување на ваквите мерки сè до моментот на случување на некој сериозен инцидент. Соодветни мерки за реакција по инциденти мора да се воспостават во организациите без разлика дали тие се во рамките на одредена сертификација или организацијата следи препораки од ИТ компании како најдобри практики. За пример можеме да го земеме Микрософт кој во својата веб библиотека ја има обработено оваа тема и нуди бесплатни совети и најдобри практики во воспоставување на неопходните безбедносни политики и стратегии [31]. Како најважни теми поврзани со оваа област кои ги споредуваме како применети во разгледаните стандарди се планирање, комуникација, анализа намалување на последиците и постојано обновување истите табеларно се прикажани во Табела 8.

Планирање: Процесите и процедурите за реакција се извршуваат и одржуваат со цел да се осигури навремена реакција по откриените безбедносни инциденти	Извршување на план за реакција по настан	COBIT 5 BAI01.10
		ISO/IEC 27001:2013 A.16.1.5
		Услови за сертифицирање 5.3.1, 5.3.2, 5.3.4 5.3.5
Комуникација и координација: Активностите за реакција се	Персоналот ги знае своите улоги и редоследот на операциите кога реакција е	ISO/IEC 27001:2013 A.6.1.1, A.16.1.1
		COBIT 5 не

координираат со внатрешните и надворешните засегнати страни и по потреба се вклучува надворешна поддршка од државни агенции за спроведување на законско дефинирани постапки	потребна	Услови за сертифицирање 5.1, 5.3
	Постојано известување за инцидентите согласно воспоставените критериуми	ISO/IEC 27001:2013 A.6.1.3, A.16.1.2
		COBIT 5 не
		Услови за сертифицирање не
	Споделување на информациите е во согласност со плановите за реакција	ISO/IEC 27001:2013 A.16.1.2
		COBIT 5 не
		Услови за сертифицирање не
Анализа: Се извршува анализа за да се осигуриме дека ќе спроведеме соодветни активности за реакција и интервенција за обновување	се извршува проверка и анализа на нотификациите од системите за детекција	COBIT 5 DSS02.07
		ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5
		Услови за сертифицирање 5.5
	Влијанието од настанатиот инцидент е јасно протолкувано и разбрано	COBIT 5 не
		ISO/IEC 27001:2013 A.16.1.6
		Услови за сертифицирање 5.2.4, 5.2.5, 5.2.6
	Извршување на форензика	COBIT 5 не
		ISO/IEC 27001:2013 A.16.1.7
		Услови за сертифицирање не
	Инцидентите се категоризирани и во согласност со плановите за реакција	COBIT 5 не
		ISO/IEC 27001:2013 A.16.1.4
		Услови за сертифицирање 5.2.4
Намалување на негативните ефекти: Се преземаат активности за да се спречи натамошно негативно зголемување на ефектот од инцидентот.	Ставање под контрола на инциденти	COBIT 5 не
		ISO/IEC 27001:2013 A.16.1.5
		Услови за сертифицирање 5.1, 5.2
	Ублажување на ефектите од инцидентите	COBIT 5 не
		ISO/IEC 27001:2013 A.12.2.1, A.16.1.5
		Услови за сертифицирање 5.2.9 , 5.4
	За новооткриените ранливости се врши ублажување на ефектите или истите се документираат како прифатливи ризици	COBIT 5 не
		ISO/IEC 27001:2013 A.12.6.1
		Услови за сертифицирање 5.5, 5.3.3
Ажурирање: Активностите за одговор и	Во плановите за реакција се вклучува ново	COBIT 5 BAI01.13
		ISO/IEC 27001:2013 A.16.1.6

реакција се подобруваат со вклучување на стекнатото искуство од сегашните и минатите реакции по инциденти.	стекнатото искуство	Услови за сертифицирање не

Табела 8: Споредба на обработуваните стандарди во областа на реакција

Table 8: Comparative table of the discussed standards in the area of respond

5.1.5 Обновување по инциденти

Оваа тема на обновување по инцидент всушност е и најкритична, бидејќи ние како професионалци и да имаме воспоставено соодветни планови за заштита, превенција и идентификација доколку немаме план што да правиме во случај сите претходни да потфрлат тогаш нема да можеме да го вратиме системот во првобитната состојба. Главна цел на организацијата е сервисите да функционираат нормално дури и по настанат инцидент, затоа администраторите мора по настанат инцидент да имаат воспоставено процедури со кои ќе го вратат системот во нормална функционалност, и по можност ќе преземат мерки за таков тип на инцидент да биде спречен во иднина. Во оваа област мора да се опфатат темите за планирање за обнова на сервисите кои биле загрозени, потоа постојано ажурирање на процесите за обнова, и комуникација и односи со засегнатите страни нивната застапеност во дискутираните стандарди е прикажана во Табела 8.

Планирање на обновување: Процесите и процедурите за обновување се извршуваат и одржуваат за да се осигури навремено враќање на функција на системите или уредите кои се засегнати од ИКТ безбедносниот настан	Извршување на планови за обновување по настан	COBIT 5 DSS02.05, DSS03.04
		ISO/IEC 27001:2013 A.16.1.5
		Услови за сертифицирање 5.2, 5.3.4, 5.3.5
Ажурирање на плановите: Плановите и процесите постојано се подобруваат и во нив се пренесува новостекнатото искуство како идни активности	Во плановите за обновување се вклучува новостекнатото искуство	COBIT 5 BAI05.07
		ISO/IEC 27001:2013 не
		Услови за сертифицирање 5.2.8
	Стратегиите за обновување редовно се ажурираат	COBIT 5 BAI07.08
		ISO/IEC 27001:2013 не
		Услови за сертифицирање не
Комуникација: Активностите за обновување се координираат со внатрешните и	Менаџирање на односи со јавноста	COBIT 5 EDM03.02
		ISO/IEC 27001:2013 не
		Услови за сертифицирање не

надворешните засегнати страни, како интернет провајдери, сопственици на нападнатите системи, производители, добавувачи, центри за координација и сл.	Се води грижа за поправка на угледот на организацијата по несакан инцидент	COBIT 5 MEA03.02
		ISO/IEC 27001:2013 не
		Услови за сертифицирање не

Табела 9: Споредба на обработуваните стандарди во областа на обновување по инциденти

Table 9: Comparative table of the discussed standards in the area of recovery

Од компарацијата може да ја утврдиме следнава анализа:

- во областа на **Идентификација** се опфатени 23 услови при што *Cobit 5* рамката исполнува 21 услов, *ISO/IEC 27001:2013* 15,5 услови и сертификација на ИС согласно Закон за електронско управување 12 услови.
- Во областа **Заштита** се опфатени 33 услови при што *ISO/IEC 27001:2013* исполнува 32 услови, *Cobit 5* рамката 29 услови и сертификација на ИС согласно Закон за електронско управување 15.5 услови.
- Во областа **Откривање-детекција** се опфатени 9 услови при што *ISO/IEC 27001:2013* исполнува 8 услови, *Cobit 5* рамката 8 услови и сертификација на ИС согласно Закон за електронско управување 4 услови.
- Во областа **Реакција** се опфатени 12 услови при што *ISO/IEC 27001:2013* исполнува 10 услови, *Cobit 5* рамката 5 услови и сертификација на ИС согласно Закон за електронско управување 4 услови.
- Во областа **Обновување по инциденти** се опфатени 5 услови при што *ISO/IEC 27001:2013* исполнува 1 услов, *Cobit 5* рамката 5 услови и сертификација на ИС согласно Закон за електронско управување 2 услови.

Сумарно од вкупно анализирани 76 услови стандард кој има најголем опфат во овие области е Cobit 5 рамката со исполнети 68 услови, потоа следи *ISO/IEC 27001:2013* со исполнети 66.5 услови и сертификација на ИС согласно Закон за електронско управување која исполнува 37.5 услови. Може да се утврди дека *Cobit 5* рамката има значителна предност во последната област **Обновување по инциденти** истото се отсликува и во видот на стандардот кој го претставува односно сеопфатен стандард за една организација која покрај безбедноста, приоритетите ги влече и од останатите стратешки заложби на организацијата.

Напомена: Компарацијата и анализата на стандардите и сертификатите е вршено самостојно базирано на лична перцепција од изучуваниот материјал, работното искуство и анализи на претходни верзии на стандардите исклучиво во делот на бодувањето, при што вредност од 0.5 се доделува само во случаи кога оценуваме дека делумно е исполнет условот.

6. Мислења и препораки

Во овој труд ги проучивме трите стандарди/сертификати при што од анализата на нивните разлики и сличности можеме да извлечеме одредени препораки и размислувања. Замислата е дел од овие препораки во рамките на надлежностите и можностите на своето работно место како ставови да се пренесат и до органите надлежни за законската регулатива во Р.М. во консултација со интересите на органот кој го претставувам.

Препорака 1. Процесот на сертификација на ИС треба да опфати измена со која не би се сертифицирал секој информациски систем посебно туку организацијата која е одговорна за функционирање на системот, каде што за секој нов воспоставен систем би се дефинирале дополнителни проверки за исполнетост на условите, со цел да се намали формалноста и ризикот од губење на сертификатот.

Мислење 1. Сертифицирањето на Информациски систем наликува и содржи елементи слични со на системот за менаџмент со информациона безбедност од *ISO/IEC 27001* стандардот. Ова мислење се базира врз основа на дел од точките за исполнетост од 3.3.1 Условите за сертификација, поспецифично точка 5.2 од условите во целост соодветствува со *PDCA* моделот. Дополнителна сличност постои и во делот 3.Барање за оценка и управување на ризикот од условите за сертификација каде се бара органот да има воспоставено структуриран пристап во управување со ризиците. (Се побарува документација, план со кој се потврдува воспоставување на структуриран пристап за управување со ризици, се идентификуваат соодветните акции на менаџментот, се дефинираат можните ресурси, одговорности и приоритети за управување со ризиците).

Мислење 2. Сертификацијата согласно Законот за електронско управување не подразбира исполнување на Стандард. Односно, доколку се сертифицира органот се добива сертификат дека се исполнети условите за сертификацијата, но не и исполнување на стандардот. Процесот на сертификација и стандардизација мора да бидат различни во спротивно доколку во законот беше пропишано дека со сертификацијата се исполнува услови за стандард за ИС тогаш истата треба и да е усогласена со условите од Законот за стандардизација и подзаконските акти.

Мислење 3. Со доставување на барањето за сертификација Органот самостојно одлучува која документација ќе ја приложи, но потребно е да го дефинира опсегот односно да се прикаже инфраструктура, да се опишат хардверските и софтверските елементи, функционалностите (услуги) на системот, опис на мрежата, документација за човечки ресурси за да се утврдат капацитетите на органот. Веќе од самото барање може да се утврдат сличности како и кај претходно опишаната *ISO* сертификација, имено кај менаџмент системот за информациона безбедност исто така го специфицираме опсегот.

Мислење 4. Во Правилникот за сертифицирање од Законот за електронско управување во став 2 од членот 4 се дава можност за утврдување на исполнетост на условите за сертификација да се утврдува и од друго правно лице определено од Министерството. Ова дава простор за слободно толкување дека во иднина може да се

очекува зголемување на обемот на сертифицирање на ИС, а следствено и делегирање на надлежноста за проверка на истите на други правни лица. За споредба доколку историски се следи процесот за регистрација на веб страници, кои во минатото ги извршуваше МАРНЕТ во рамките на Министерството сега се извршуваат од приватни компании со овластување.

Препорака 2. Законот за електронско управување и подзаконските акти во делот на сертификација на ИС во голема мера соодветствуваат со *ISO/IEC 27001* стандардот но верзијата 2005. При што слично како и кај верзијата на стандардот условите односно проверките од Анекс А се задолжителни. Условот од 4.4 како механизам за идентификација да се користи електронски потпис издаден од владина инфраструктура на јавен клуч и при издавање на електронскиот потпис направена е физичка потврда за идентитет на лицето е неприменлив во праксата бидејќи ниту еден орган не го исполнува, единствено официјално издавање на клуч од владина инфраструктура се користи при здравствените картички, а и таа услуга не е во целост бидејќи не е извршена физичка потврда на идентитетот на лицето. Потребна е измена на легислативата во одредени делови посебно во условите за сертификација да соодветствуваат со верзијата 2013 од стандардот каде што сите услови за сертификација не се задолжителни туку се препорачани за користење.

Препорака 3. Во Законот за електронско управување не е дефинирано што се случува со информацискиот систем доколку органот го изгуби сертификатот? Дали услугата која органот ја нуди кон граѓаните треба да биде прекината или органот свесно ќе презема ризик да го опслужува системот согласно законските надлежности ? Сметам дека треба да се дополнат подзаконските акти да опфатат ваков случај, и истите да содржат насоки на органите како да постапуваат во случај на губење на сертификатот.

7. Заклучок

Овој магистерски труд прикажува процес на компаративна анализа помеѓу *ISO*27001:2013 сертификација, *COBT 5* методологијата и сертификацијата на информациони системи утврдена со Законот за електронско управување. Дополнително во целост е опишан процесот на сертификацијата на информациони системи која согласно законот се однесува за државните органи и органите кои вршат услуги по електронски пат во Република Македонија.

Со овој труд беа истражени, утврдени и прикажани сличностите, но и разлики во процесите при што може да се извлечат следниве поважни заклучоци:

- Со ISO/IEC 27001 стандардот и COBIT работната рамка се сертифицира дадена компанија и истата добива еден сертификат кој потврдува дека таа го исполнува стандардот. Со сертификацијата на ИС согласно Законот за електронско управување се сертифицира информациски систем на дадена државна институција, секој посебно, така да може да се случи една државна институција да има посебни сертификати за неколку нејзини информациски системи;
- Сертификацијата согласно Законот за електронско управување не подразбира исполнување на некој стандард. Односно, државниот органот при сертификација добива сертификат дека се исполнети условите за сертификацијата, но не и дека е исполнет некој стандард;
- Сертификацијата согласно Законот за електронско управување се базира најмногу врз делови од ISO/IEC 27001:2005, а во помала мера и делови од ISO/IEC 27002, и ISO/IEC 27005;
- Меѓународните стандарди се постојано изложени на нови позитивни практики и искуства и постојано следат своевиден процес на еволуција, подновување со постојните трендови, односно носење на нови верзии од истите. За споредба Законот за електронско управување и подзаконските акти ретко трпи измени или измените се минимални. Од 2009 година кога е донесен, до сега, само три пати минимално е изменет во 2011, 2015 и 2016.
- Во ISO/IEC 27001 и COBIT постои процес на т.н. постојано подобрување на процесите – созревање на процесите, додека во македонската легислатива ова отсуствува. Дополнително во COBIT постои и делумно исполнување на процесот, односно се утврдува на кое ниво бил процесот и на кое ниво

раководството одлучило да биде понатаму, додека во ISO/IEC 27001 и во македонскиот стандард постои само исполнува или не исполнува.

- Процесот на сертификација на ИС од Законот за електронско управување се однесува исклучиво за државните институции и заради тоа истиот не се наплаќа што може да се смета како предност пред обезбедување на друг меѓународен стандард. На пример, процесот на сертификација со ISO 27001 стандардот за организација со 50 до 70 вработени може да чини и до 50 илјади долари.
- Законот за електронско управување не го уредува само сертифицирањето на информацискиот систем, туку се грижи и истиот да е ускладен и со други правни прописи. Тоа може да се види од "Изјавата за взаемна доверливост на податоци" која преставува усогласување со Законот за лични податоци. Ова е во согласност со препораката за усогласување со законската регулатива и други договорни обврски на ISO/IEC 27001 сертификацијата.
- Во Законот за електронско управување никаде не е ставена временска рамка за ресертификација на веќе сертифициран информациски систем, освен во случај на негова измена. Ова е различно од останатите стандарди, на пример, кај ISO/IEC 27001 стандардот, работната организација треба да се ресертифицира на секои три години.
- Во Законот за електронско управување не е дефинирано што се случува со информацискиот систем доколку на органот му е одземен сертификатот. Дали услугата која органот ја нуди кон граѓаните треба да биде прекината или органот свесно ќе преземе ризик и ќе продолжи да го опслужува системот согласно законските надлежности? Потребно е да се дополнат подзаконските акти да опфатат и ваков случај, и истите да содржат насоки на органите како да постапуваат во случај на одземање на сертификатот.
- Во македонската регулатива покрај сертификација на системот има и друг процес на евиденција на ИС, кој го извршува Министерството за информатичко општество и администрација. Министерството согласно законот води регистар. За истиот е должен да се грижи вклучувајќи и креирање на редовна заштитна копија на податоците, вклучувајќи ја и документацијата поврзана со имплементацијата од проектите поврзани со ИКТ. Обврската пак за чување на

документацијата поврзана со системот во ISO/IEC 27001 сертификација ја има организацијата и истата е услов за исполнување.

- Согласно Законот за електронско управување се укажува на Министерството за информатичко општество и администрација да го утврди процесот на сертифицирање, проверка и контрола над функционалноста на информациските системи кои ги користат државните органи.
- Со доставување на барање за сертификација државниот орган самостојно одлучува која документација ќе ја приложи, што не е најдобро решение. Потребно е органот да го дефинира опсегот односно да се прикаже инфраструктура, да се опишат хардверските и софтверските елементи, функционалностите на системот, да има документација за човечки ресурси, се со цел да се утврдат капацитетите на органот.
- Целиот процес сертификација кај ISO/IEC 27001 стандардот може да трае од 5 до 24 месеци, додека информациските системи на државните институции се сертифицираат за 1 месец, доколку се исполнети сите законски услови.

Овој магистерски труд имаше тенденција да покаже дека користењето на стандарди во ИТ индустријата е секогаш препорачано, бидејќи истите се испробани алатки кои нудат ефективни акции и најдобри практики за зголемување на сигурноста во областа на ИТ. Стандардите и добрите практики на организациите им овозможуваат широка палета на опции и усовршување во согласност со нивните специфични потреби. Истражувањата поврзани со овој труд ми покажа дека во ИТ индустријата не само што се среќава имплементирање на повеќе сродни стандарди туку истото и се препорачува од експертите. Од овој труд може да увидиме дека *COBIT* методологијата опфаќа поголем спектар на области што се среќаваат во една организација додека ISO/IEC 27001 и сертификација на ИС согласно закон е тесно специфицирана и поврзана во областа на ИТ безбедност и менаџирање со ИТ ризици.

Овој факт ни покажува дека истите може да се комбинираат во одредени делови, но и да се дополнат таму каде што одреден стандард има недостаток. Сметам дека проучените стандарди ни ги овозможуваат сите неопходни елементи за развој и планирање на информационата безбедност, истите се лесно прилагодливи за примена на најдобри практики, ни овозможуваат да внесеме рамка на ИТ безбедноста во постојните развојни стратегии на организациите, ни обезбедуваат ред во управувањето, надгледувањето и менаџирањето со ИТ. Истовремено овие стандарди ни помагаат да го минимизираме ризикот или да менаџираме во прифатливи рамки, и сето ова со една цел да го заштитиме она што е најважно во една организација – информацијата.

8. Користена литература

[1] Mc Afee (2014) *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II.* Center for Strategic and International Studies.

[2] ISO/IEC (2010) ISO/IEC 27000 - *An Introduction to ISO/IEC 27001 (ISO27001), ISO/IEC 27000 - ISO/IEC 27001 and ISO/IEC 27002 Standards*. Преземено на 01.11.2016 од http://www.27000.org/iso-27001.htm

[3] ISACA (2012) *COBIT 5 framework*. Преземено на 01.11.2016 од http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx

[4] Собрание на РМ (2016) *Закон за електронско управување*. Службен весник на Република Македонија, бр. 105 од 21.08.2009 година, последна измена и дополнување од 18.03.2016.

[5] BH Consulting (2006) *BS 7799 becomes ISO 27001*. Преземено на 01.11.2016 од http://www.bhconsulting.ie/BS%207799%20becomes%20ISO%2027001.pdf

[6] ISO/IEC (2005) *ISO/IEC 17799:2005 - Information technology -- Security techniques -- Code of practice for information security management*. Преземено на 01.11.2016 од http://www.iso.org/iso/catalogue_detail?csnumber=39612

[7] ISO (2014) *ISO/IEC 27000:2014.* Преземено на 01.11.2016 од https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en

[8] Ochel D. (2014) *Comparing NIST's Cybersecurity Framework with ISO/IEC 27001.* SECUILIBRIUM, LLC.

[9] Donovan, K., and WIldman, B. (2012) *IT Security Frameworks - ACG 6415.* Преземено на 01.11.2016 од https://acg6415.wikispaces.com/file/view/IT_Security_Frameworks+2.pptx

[10] Собрание на Р. М. (2015) *Закон за градење*. Службен весник на Република Македонија, бр. 130 од 28.10.2009 година,п оследна измена и дополнување од 11.12.2015.

[11] Собрание на Р. М. (2008) *Закон за податоци во електронски облик и електронски потпис*. Службен весник на Република Македонија. 34/01, 06/02, 98/08

[12] Собрание на Р. М. (2008) *Закон за заштита на личните податоци*. Службен весник на Република Македонија бр. 7/05 и 103/08

[13] Министерство за информатичко општество и администрација на Р. М. (2010) *Правилник за начинот на сертифицирање на информациските системи и за формата и содржината на сертификатот*

[14] Arora, B. (2010) *Comparing different information security standards: COBIT v s. ISO/IEC 27001.* Преземено на 01.11.2016 од Carnegie Mellon University, Qatar https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf

[15] Конференции и обуки за стратешки области на ИКТ безбедност ISACA (2016) *(Information Systems Audit and Control Association).* преземено од http://www.isaca.org/cyber-conference/sessions.html

[16] García M. M. T. (2005) *ISO/IEC 27002 vs. COBIT: Security Information Planning.* Преземено на 01.11.2016 од http://www.isaca.org/Groups/Professional-English/iso-iec-27000-series/GroupDocuments/Article%20ISO%2027002%20vs%20COBIT%20Info%20Sec%20Plan%20-%20ISACA.pdf

[17] Институт за акредитација на Република Македонија (2014) *Услови за акредитација.*

[18] Собрание на Р.М. (2014) *Закон за стандардизација на Р.М.* Сл. Весник на РМ. Бр.54/2002,84/2012,23/2013, 41/2014.

[19] ISO (2014) *ISO/IEC 27K timeline.* Преземено на 01.11.2016 од http://www.iso27001security.com/html/timeline.html

[20] NIST (2007) NIST Special Publications. Преземено на 01.11.2016 од http://csrc.nist.gov/publications/PubsSPs.html

[21] SOX (2006) A Guide To The Sarbanes-Oxley Act. Преземено на 01.11.2016 од http://www.soxlaw.com/

[22] Committee of Sponsoring Organizations of the Treadway Commission (2015) *COSO guidance*. Преземено на 01.11.2016 од http://www.coso.org/guidance.htm

[24] ISO (2014) *The ISO Survey*. Преземено на 01.11.2016 од http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO/IEC% 27001

[25] ISO/IEC (2015) *ISO/IEC Directives, Part 1, Consolidated ISO Supplement.* 6th Edition. Преземено на 01.11.2016 од https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/annex_sl_excerpt_-_2015__6th_edition_-hls_and_guidance_only.pdf

[26] Sheikhpour, R., and Modir, N. (2012). *An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls*. International Journal of Security and Its Applications 6(2), pp. 13-28.

[27] Disterer, G. (2013) *ISO/IEC 27000, 27001 and 27002 for Information Security Management.* Journal of Information Security 4(2), pp. 92-100.

[28] Verry, J. (2016) *How much does ISO 27001 Certification Cost.* PivotPoint Security. Преземено на 01.11.2016 http://www.pivotpointsecurity.com/blog/iso-27001-cost-estimate-48000-information-security-confidence-priceless/

[29] Microsoft (2016) *Identifying Risks in Operations*. Преземено на 01.11.2016 https://technet.microsoft.com/en-us/library/cc535338.aspx

[30] Kruegel, C., Valeur, F., and Vigna, G. (2005) *Intrusion Detection and correlation: challenges and solutions*. Advances in Information Security, vol 14, Springer US. ISBN: 978-0-387-23398-7

[31] Microsoft (2016) *Responding to IT Security Incidents*. Преземено на 01.11.2016 од https://technet.microsoft.com/en-us/library/cc700825.aspx

[32] Cichonski, P., Millar, T., Grance, T., and Scarfone, K. (2012) *Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology*. Special Publication 800-61 Revision 2, NIST.

[33] Министерство за транспорт и врски на Р. Македонија (2011) *Уредба за минималните технички стандарди и услови во поглед на опремата (хардверот), како и функционалноста на софтверот за електронското јавно наддавање согласно Законот за градежно земјиште усвоена на седница на Влада на Р.М.* 26.07.2011 Службен весник на Република Македонија бр. 17/2011 и 53/2011.

[34] BSI (2016) *Our history*. Преземено на 01.11.2016 од http://www.bsigroup.com/en-GB/about-bsi/our-history/

[35] Brotby, W.K., and Hinson, G. (2013*) PRAGMATIC Security Metrics: Applying Metametrics to Information Security.* Auerbach Publications, ISBN-13: 978-1439881521.

[36] Kuligowsk, C. (2009) *Comparison of it security standards.* White paper. Преземено на 01.11.2016 од http://www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf

[37] Onifade, O. (2015) *Implementing an ISO-integrated Management System Using COBIT 5.* COBIT Focus.

[38] Bailey, E., and Becker, J. D. (2014) *A Comparison of IT Governance and Control Frameworks in Cloud Computing.* In Proceedings of the 20th Americas Conference on Information Systems (AMCIS), Savannah Georgia USA.

[39] Magnusson, C. (2007*) Corporate Governance, Internal Control and Compliance.* Technical Report from Confederation of Swedish Enterprise.

[40] ISACA (2012) *COBIT 5 Information Security.* An ISACA Framework.

ПРИЛОГ 1

П Р А В И Л Н И К
ЗА НАЧИНОТ НА ПРАВЕЊЕ НА СИГУРНОСНА КОПИЈА, АРХИВИРАЊЕ И ЧУВАЊЕ, КАКО И ЗА ПОВТОРНО ВРАЌАЊЕ НА ЗАЧУВАНИТЕ ЛИЧНИ ПОДАТОЦИ

Член 1

Со овој Правилник се пропишува начинот на правење на сигурносна копија, архивирање и чување, како и за повторно враќање на зачуваните лични податоци кои се обработуваат во ОРГАНОТ (во понатамошниот текст: ОРГАНОТ).

Член 2

ОРГАНОТ задолжително врши редовно снимање на сигурносна копија и архивирање на податоците во информацискиот систем на начин на кој се гарантира постојана можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

За да се спречи губење или уништување на податоците се користи сервер за поддршка во кои еднаш дневно се креира резервна копија на личните податоци кои се обработуваат во Дирекцијата во случај на пад на компјутерскиот систем или негово оштетување од каква било причина, сите податоци остануваат сочувани на серверот.

Податоците во резервната копија се енкриптираат пред да се префрлат на серверот. Во серверот се поставени цврсти дискови (hard disc) во RAID конфигурација така што и при дефект на некој од дисковите нема губење на информациите.

Администраторот на информацискиот систем еднаш неделно задолжително ја проверува функционалноста на сигурносните копии од став 1 на овој член за што писмено го известува Офицерот за заштита на личните податоци и Извршниот директор на ОРГАНОТ.

Член 3

Заради заштита од неовластен пристап, серверот за поддршка во кој е сместена сигурносна копија на сите снимени податоци е сместен во безбедна просторија заштитена со сигурносна брава до која имаат пристап само администраторот на информацискиот систем.

Член 4

Контролорот задолжително прави сигурносни копии секој работен ден и на крајот од работната седмица, а по потреба и секој последен работен ден во месецот.

Сигурносните копии се прават на начин што се гарантира постојана можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

Задолжително прави дополнителна сигурносна копија на податоците од серверот за поддршка на медиум, на крајот од работната недела и секој последен работен ден во месецот.
Направената сигурносна копија од став 1 на овој член, подлежи на физичка и криптографска заштита, со што се оневозможува каква било модификација на содржината на истата.
По извршеното копирање на личните податоци содржани во електронските документи, сигурносната копија се носи на друга оддалечена безбедна локација која се наоѓа надвор од просторијата во која се чуваат серверите или персоналните компјутери во кои се сместени збирките на личните податоци за кои се прави сигурносна копија.
Сигурносните копии коишто се чуваат на друга одалечена локација од местото каде е сместен информацискиот систем ќе бидат заштитени со соодветни технички и организациски мерки.
Меѓусебните права и обврски на контролорот и правното, односно физичкото лице каде да се чуваат сигурносните копии ќе се уредат со писмен договор во којшто задолжително ќе бидат содржани техничките и организациските мерки за обезбедување тајност и заштита на личните податоци.
Пристап до оддалечената безбедна локација каде се чува медиумот имаат само овластени лица од контролорот, при што медиумот се чува затворен во сеф со безбедносна брава и кој е обезбеден од физички влијанија (кражба, пожар, поплава и други влијанија).
Обезбедувањето на безбедната локација од став 3 на овој член го врши Извршниот директор на ОРГАНОТ.
Администраторот на информацискиот систем задолжително ја проверува функционалноста на сигурносните копии од став 1 на овој член за што писмено го известува Офицерот за заштита на личните податоци и Извршниот директор на ОРГАНОТ

Член 5

При повторно враќање на зачуваните лични податоци, се врши евидентирање на повторното враќање на податоците, како и се евидентира датумот на враќањето на податоците, категориите на податоците кои се вратени.
За враќањето на личните податоци се составува записник во кој се наведува лицето кое го врши враќањето, времето и категоријата на личните податоци

Член 6

Овој Правилник влегува во сила и истиот ќе се применува од денот на неговото донесување.