



Факултет за информатику и менаџмент

**Ревизија информационих и
комуникационих технологија**

Магистарски рад

Ментор:

Доцент др Гојко Грубор

Кандидат:

Радуле Шошкић
(индекс бр. I-6/2005)

Сажетак

Овај рад се бави ревизијом примене и коришћења информационих и комуникационих технологија. Он даје шири преглед теорије и праксе у овој области, укључујући и неке конкретне примере и препоруке. Посебно је размотрен однос између традиционалне, финансијски оријентисане ревизије и савремене, техничко-технолошки оријентисане ревизије. Истакнуте су предности и недостаци оба приступа и дискутована могућност и евентуалне користи од њихове комбинације – интегрисане ревизије – у којој би се ујединиле предности ова два приступа.

Кључне речи:

ревизија, ревизор, контрола, ризик, систем интерних контрола, интерна ревизија, технолошка ревизија, ревизија информационих технологија, ревизија информационих система, ревизија информационих и комуникационих технологија, технолошки ревизор, ревизор информационих технологија, ревизор информационих система, ревизор информационих и комуникационих технологија, пословни ризик, интерна контрола, опште контроле, генералне контроле, апликативне контроле.

Abstract

This paper deals with auditing of application and use of information and communication technologies. It gives a broad overview of both theory and practice, including some examples and advice. Particularly, the paper considers the relation between traditional, financial statement oriented auditing, and modern, more technologically and technically oriented auditing. It underlines the advantages and deficiencies of both, and discusses possible benefits of a joint, integrated approach, which would incorporate the best of the two worlds.

Keywords:

audit, auditor, control, risk, internal control system, internal audit, technology audit, information technology audit, information systems audit, information and communication technology audit, technology auditor, information technology auditor, information systems auditor, information and communication technology auditor, business risk, internal control, general control, application control.

ПРЕГЛЕД СЛИКА

Слика 1: Интерне контроле у ИКТ системима.....	24
Слика 2: Животни циклус технолошке ревизије.....	28
Слика 3: Подручја обухваћена техничким контролама.....	36
Слика 4: Три димензије CobiT приступа.....	50
Слика 5: Напад на апликациони сервер.....	72
Слика 6: Напад на сервер продукционе базе података.....	73
Слика 7: Ескалација напада.....	75

ПРЕГЛЕД ТАБЕЛА

Табела 1: Дефиниције интерне ревизије у периоду 1990-2009.....	88
Табела 2: FIPS стандарди.....	93
Табела 3: Архивирани FIPS стандарди.....	97

САДРЖАЈ

1. МЕТОДОЛОГИЈА ИСТРАЖИВАЧКОГ РАДА.....	1
1.1. ОБРАЗЛОЖЕЊЕ ИСТРАЖИВАЧКОГ РАДА И ПРЕТХОДНА ИСТРАЖИВАЊА.....	1
1.2. ПРЕДМЕТ РАДА.....	1
1.3. ХИПОТЕТИЧКИ ОКВИР.....	2
1.3.1. Општа хипотеза.....	2
1.3.2. Појединачне хипотезе.....	2
1.4. ЦИЉЕВИ ИСТРАЖИВАЊА.....	2
1.4.1. Научни циљ.....	2
1.4.2. Конкретни циљ.....	3
1.5. ТОК ИСТРАЖИВАЧКОГ ПРОЦЕСА И МЕТОДИ ИСТРАЖИВАЊА.....	3
1.5.1. Ток истраживачког процеса.....	3
1.5.2. Општи научни методи.....	3
1.5.3. Логички методи.....	3
1.5.4. Статистички методи.....	3
2. РЕВИЗИЈА ИНФОРМАЦИОНИХ ТЕХНОЛОГИЈА.....	4
2.1. УВОД.....	4
а) Ревизија информационих технологија настала у контексту традиционалне (или конвенционалне) ревизије.....	5
б) Ревизија информационих технологија настала у контексту самих информационих технологија.....	6
2.2. ОСНОВНИ ПОЈМОВИ – МЕСТО И УЛОГА РЕВИЗИЈЕ.....	7
2.2.1. Дефиниција интерне ревизије.....	7
2.2.2. Независност и објективност интерне ревизије.....	7
2.2.3. Професионална етика.....	9
2.2.4. Место и улога интерне ревизије.....	10
2.3. МЕСТО И УЛОГА ТЕХНОЛОШКЕ РЕВИЗИЈЕ.....	11
2.3.1. Настанак и историјат технолошке ревизије.....	11
2.3.2. Дефиниција технолошке ревизије.....	12
2.3.3. Место технолошке ревизије у организацији и линија одговорности.....	13
а) Технолошка ревизија као део функције интерне ревизије.....	13
б) Технолошка ревизија као део функције за технику/технологије (ИТ, ИКТ).....	14
в) Технолошка ревизија као део функције корпоративне или ИТ безбедности.....	14
г) Екстерна технолошка ревизија.....	15
2.3.4. Специфична независност и објективност технолошке ревизије.....	16
а) Интерна технолошка ревизија.....	16
б) Екстерна технолошка ревизија.....	17
2.4. РИЗИЦИ И КОНТРОЛЕ У ОБЛАСТИ ПРИМЕНЕ И КОРИШЋЕЊА ИНФОРМАЦИОНИХ И КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА.....	18
2.4.1. Пословни ризици.....	18
2.4.2. Ревизорски ризици.....	18
2.4.3. Информатички ризици.....	19
2.4.4. Мрежни и комуникациони ризици.....	21
2.4.5. Контроле и системи интерних контрола у ИКТ.....	23
2.4.6. Класификација интерних ИКТ контрола.....	23
2.5. ПРОЦЕС РЕВИЗИЈЕ И РЕВИЗОРСКЕ АКТИВНОСТИ.....	27
2.5.1. Животни циклус процеса ревизије.....	27
2.5.2. Процена ризика.....	27
2.5.3. Планирање.....	29
2.5.4. Израда програма ревизије.....	30
2.5.5. Упознавање са предметом ревизије.....	30

2.5.6. Прелиминарно истраживање.....	31
2.5.7. Рад на терену.....	31
2.5.8. Извештавање.....	32
2.5.9. Праћење по извештају.....	32
2.5.10. Конвенционални и стриктно технолошки приступ – главне разлике и могућност интеграције.....	33
а) Разлике у третману процене ризика.....	33
б) Системски приступ и приступ путем једнократне пробе (истраге).....	34
в) Неформална и континуална ревизија.....	34
г) Провере и тестови.....	35
2.6. ПОСЕБНЕ ОБЛАСТИ ТЕХНОЛОШКЕ РЕВИЗИЈЕ.....	37
2.6.1. Ревизија информатичке безбедности	37
2.6.2. Ревизија преварних радњи и место дигиталне форензике у технолошкој ревизији	38
2.6.3. Ревизија усклађености.....	38
2.6.4. Самооцењивање.....	39
2.7. РЕВИЗОРСКИ АЛАТИ.....	40
2.7.1. Општи ревизорски алати – рачунарска подршка ревизији.....	40
а) ACL.....	40
б) IDEA (CaseWare IDEA Inc.).....	40
в) Reliant Auditor (Reliant Solutions, Inc.).....	41
г) TopCAATs (Reinvent Data Ltd).....	41
д) ActiveData (InformationActive).....	41
ђ) Monarch Professional (Datawatch).....	41
е) Програми за опште статистичке намене.....	42
2.7.2. Специјализовани ревизорски алати – рачунарска подршка технолошкој ревизији.....	42
а) Мапирање мрежа.....	42
б) Анализа бежичних мрежа.....	43
в) Идентификовање слабости система.....	43
г) Ескалација привилегија	43
д) Пробојни тестови.....	44
ђ) Анализа трослојних апликација	44
е) Анализа ИП телефоније (VoIP).....	44
ж) Дигитална форензика.....	44
з) Пакети и дистрибуције.....	45
2.8. ПРОФЕСИОНАЛНА КОМПЕТЕНЦИЈА ТЕХНОЛОШКИХ РЕВИЗОРА	45
2.8.1. Техничка знања.....	45
2.8.2. Општа пословна и ревизорска знања.....	46
2.8.3. Социјалне вештине и способности.....	46
2.8.4. Перманентна едукација и професионална сертификација.....	47
2.9. ПРОФЕСИОНАЛНА РЕГУЛАТИВА – СТАНДАРДИ, ПРЕПОРУКЕ И РАДНИ ОКВИРИ.....	47
2.9.1. Стандарди Института интерних ревизора	47
2.9.2. Стандарди Асоцијације за ревизију и контролу информационих система (Information Systems Audit and Control Association – ISACA).....	48
а) Стандарди.....	48
б) Управљачке смернице	49
2.9.3. Стандарди COSO.....	52
а) Оквир за интерну контролу и управљање.....	52
б) Оквир за управљање ризиком.....	53
2.9.4. Стандарди Међународне организације за стандардизацију (ISO).....	53
а) Стандард 27001.....	54

б) Стандард 27002.....	55
2.9.5. Стандарди НИСТ.....	56
2.9.6. Стандарди БСИ.....	56
2.9.7. Стандарди ИСФ.....	57
3. СТУДИЈА СЛУЧАЈА – ПРИМЕР РЕВИЗИЈЕ ИНФОРМАЦИОНОГ ПОДСИСТЕМА.....	59
3.1. УВОД.....	59
3.2. ОПИС СИТУАЦИЈЕ.....	59
3.3. ПРИМЕРИ ТРАДИЦИОНАЛНОГ РЕВИЗОРСКОГ ПРИСТУПА.....	61
3.3.1. Интерна ревизија – конвенционални приступ.....	61
3.3.2. Интерна ревизија – технолошки приступ.....	64
3.3.3. Екстерна ревизија.....	65
3.4. ПРИМЕР АНАЛИЗЕ УСКЛАЂЕНОСТИ СА БЕЗБЕДНОСНИМ СТАНДАРДИМА.....	66
3.5. ПРИМЕР ИНТЕГРИСАНОГ РЕВИЗОРСКОГ ПРИСТУПА.....	67
3.5.1. Делокруг и циљеви ревизорског задатка.....	67
3.5.2. Анализа архитектуре.....	67
3.5.3. Енумерација мрежних уређаја, сервера и радних станица.....	67
3.5.4. Енумерација сервиса, „скенирање портова” (port scanning).....	68
3.5.5. Идентификовање оперативних система.....	69
3.5.6. Идентификовање верзија и сервисног статуса.....	69
3.5.7. Идентификовање слабости (vulnerability scanning).....	70
3.5.8. Налази и мишљење ревизије; препоручене мере.....	71
3.6. ЕКСПЕРИМЕНТАЛНИ ТЕСТ НА ПРОБОЈ (КОНТРОЛИСАНИ НАПАД СА ЕСКАЛАЦИЈОМ).....	71
3.6.1. Мотивација.....	71
3.6.2. Контролисани напад.....	72
а) Напад на апликативни сервер.....	72
б) Напад на сервер наменске базе података.....	73
в) Напад на корисничку лозинку системског администратора.....	74
г) Напад на остале делове информационог система.....	74
3.6.3. Ескалација напада.....	75
3.7. ГЛАВНИ НАЛАЗИ СТУДИЈЕ СЛУЧАЈА.....	76
4. ДИСКУСИЈА.....	78
4.1. ДЕФИНИЦИЈА ТЕХНОЛОШКЕ РЕВИЗИЈЕ.....	78
4.2. РЕВИЗИЈА СИСТЕМА ИЛИ РЕВИЗИЈА ТЕХНОЛОГИЈА?.....	79
4.3. ТЕРМИНОЛОШКЕ ДИЛЕМЕ: ПРИЛАГОЂАВАЊЕ НЕКИХ СТРУЧНИХ ТЕРМИНА НАШОЈ КУЛТУРИ И ЈЕЗИКУ – ОБАВЕЗНО, ПОЖЕЉНО, СУВИШНО ИЛИ НЕМОГУЋЕ?.....	81
4.3.1. Governance/Management/Control.....	81
4.3.2. Firewall/Router/Switch.....	83
4.3.3. Backup/Restore.....	84
5. ЗАКЉУЧЦИ.....	85
5.1. ДУАЛИЗАМ И ПАРЦИЈАЛНИ ПРИСТУПИ У ТЕХНОЛОШКОЈ РЕВИЗИЈИ.....	85
5.2. НЕОПХОДНОСТ ИНТЕГРАЦИЈЕ.....	85
5.3. ЗНАЧАЈ ТЕХНИЧКИХ КОНТРОЛА И ОДГОВАРАЈУЋИХ СТРУЧНИХ КОМПЕТЕНЦИЈА.....	86
5.4. НЕОПХОДНОСТ ДЕФИНИСАЊА УЛОГЕ И МЕСТА ТЕХНОЛОШКЕ РЕВИЗИЈЕ.....	86
5.5. СПЕЦИФИЧНА НЕЗАВИСНОСТ И ОБЈЕКТИВНОСТ.....	87
5.6. ПОТРЕБА ЗА СТРУЧНОМ ЛИТЕРАТУРОМ.....	87
6. ПРИЛОЗИ.....	88
6.1. ДЕФИНИЦИЈЕ ИНТЕРНЕ РЕВИЗИЈЕ.....	88
6.2. ПРОФЕСИОНАЛНА РЕГУЛАТИВА (СТАНДАРДИ, ПРЕПОРУКЕ И РАДНИ ОКВИРИ).....	89

6.2.1. Регулатива Института интерних ревизора (The Institute of Internal Auditors – ИА)	89
а) The Professional Practices Framework.....	89
б) Global Technology Audit Guides – GTAG.....	89
в) Guide to the Assessment of IT Risk – GAIT.....	89
6.2.2. Регулатива Асоцијације за ревизију и контролу информационих система (Information Systems Audit and Control Association – ISACA).....	90
а) IS Standards, Guidelines and Tools and Techniques for Auditing and Assurance and Control Professionals.....	90
б) COBIT – Control Objectives for Information and Related Technologies.....	90
6.2.3. Стандарди Међународне организације за стандардизацију (ISO) и других стандардизационих организација.....	91
а) Међународни стандарди ISO/IEC.....	91
б) Амерички национални стандарди	93
в) Индустијски стандарди у приватном власништву.....	97
г) Немачки државни стандарди, упутства и друге публикације (BSI – Bundesamt für Sicherheit in der Informationstechnik).....	98
6.3. ПРОФЕСИОНАЛНА УДРУЖЕЊА И ДРУГЕ ОРГАНИЗАЦИЈЕ ОД ЗНАЧАЈА ЗА ОБЛАСТ ТЕХНОЛОШКЕ РЕВИЗИЈЕ И ИНФОРМАТИЧКЕ БЕЗБЕДНОСТИ.....	98
6.4. ПРОФЕСИОНАЛНИ СЕРТИФИКАТИ ОД ЗНАЧАЈА ЗА ОБЛАСТ ТЕХНОЛОШКЕ РЕВИЗИЈЕ И ИНФОРМАТИЧКЕ БЕЗБЕДНОСТИ.....	99
7. РЕФЕРЕНЦЕ И ЛИТЕРАТУРА.....	100

1. МЕТОДОЛОГИЈА ИСТРАЖИВАЧКОГ РАДА

1.1. ОБРАЗЛОЖЕЊЕ ИСТРАЖИВАЧКОГ РАДА И ПРЕТХОДНА ИСТРАЖИВАЊА

Област ревизије информационих технологија код нас до сада није обрађивана у стручној литератури. То је пре свега последица чињенице да се код нас овом облашћу, барем до сада, бавио врло мали број специјалиста па је стога и број потенцијалних аутора, као и број потенцијаних читалаца овакве литературе био веома мали. Оваква ситуација је дестимулисала тржишно оријентисане издаваче, тако да је издавачка делатност у овој области практично сасвим изостала.

Ипак, примећује се да у новије време код нас убрзано расте интерес за ову тему. Потребa за стручним знањима и одговарајућом литературом је све већа. У порасту је број организација које у својим структурама предвиђају одговарајуће специјализоване службе, на високим школама и факултетима се развијају курсеви из ове области, формирају се струковна удружења итд. Мотивација да се ова тема истражи и обради кроз магистарски рад углавном је заснована управо на препознавању ове потребе.

1.2. ПРЕДМЕТ РАДА

Предмет овог рада, у најширем смислу, налази се у области ревизије информационих технологија. Ревизорски приступ информационим технологијама могућ је са више аспеката. Тако, на пример, ревизија може бити оријентисана ка топологији примењеног технолошког решења, при чему се одвојено посматрају поједини сегменти мрежа, мрежни уређаји, радне станице, сервери итд. Други могући приступ дели примењену технологију по слојевима (*OSI*, *TCP/IP*). У овом приступу се ревизији подвргава сваки слој посебно: физички, мрежни, апликативни итд, што је опет зависно од примењеног модела (7-слојни *OSI*, 4-слојни итд). Даље, могући су приступи по фазама животног циклуса система, по организационим целинама, улогама и областима одговорности унутар организације, по приоритетима на основу претходно процењеног ризика, итд. При свему томе, могуће су (и у пракси веома честе) произвољне комбинације ових приступа, што даље проширује могућности и чини да конкретно опредељење по овом питању буде још сложеније.

Предмет овог рада је стога конкретно усмерен на то да се, на бази задатог хипотетичког оквира, успостави предлог одговарајућег приступа или комбинације приступа, те да се истраже применљивост, предности и недостаци, ефикасност и ефективност предложеног модела и одговарајућих ревизорских поступака, техника и алата. Крајњи резултат рада треба да пружи свеобухватан, уравнотежен и јасно структуриран преглед расположивог знања као и да сублимира и интегрише најбољу препознату теорију и професионалну праксу из ове широке области у овом тренутку.

1.3. ХИПОТЕТИЧКИ ОКВИР

1.3.1. *Општа хипотеза*

Савремена ревизија информационих технологија је професија и пословна активност око чије дефиниције, циљева и делокруга још увек није постигнут општи консенсус у стручној јавности. Позната теорија и пракса у овом тренутку још увек нуде више различитих и у извесној мери супростављених мишљења о томе. Може се показати да су савремени погледи на ревизију информационих технологија углавном окупљени око две главне групе, које су условљене својим пореклом и каснијом еволуцијом, долазе из два одвојена исходишта и имају два одвојена правца развоја. Тако се данас може говорити о две „школе” ревизије информационих технологија – једна је настала у контексту традиционалне ревизије, док се друга развила у окружењу информационих технологија.

Поред потврђених предности, основно ограничење традиционалне ревизије је у фаворизовању ревизорских приступа који полазе од организационе шеме, од поделе улога и одговорности у организацији а у новије време и од претходно процењеног ризика, док се, супротно томе, приступи који узимају за полазиште тополошке, функционалне и друге сложеније технолошке карактеристике система ретко или уопште не користе.

Други правац развоја текао је потпуно независно од конвенционалне ревизије и без икакве везе са професијом традиционалног ревизора. Он је настао као саставни део самих информационих технологија и то као исказ природне потребе да се технологија сама по себи мора подвргавати ревизији у току целог свог животног циклуса. Развој технологија и техничких решења која се на њима заснивају одувек је подразумевао и потребу за ревизијом. Све фазе животног циклуса једног ИТ решења обавезно укључују детекцију, реакцију и корекцију. У овом контексту је на природан начин дошло до препознавања потребе да се ревизија информационих технологија издвоји у посебну дисциплину у оквиру информатике и да буде прихваћена као засебна професија.

1.3.2. *Појединачне хипотезе*

Полазећи од опште хипотезе, може се показати да се оптималним комбиновањем теорије и праксе двају наведених „школа ревизије” могу превазићи њихова индивидуална ограничења и постићи значајно унапређење укупне ефикасности и ефективности ревизије информационих технологија. Наиме, могуће је показати да су ови концепти великим делом међусобно комплементарни, уз одређена преклапања, те да је изводљива значајна мера њихове интеграције, уз обострани добитак.

1.4. ЦИЉЕВИ ИСТРАЖИВАЊА

1.4.1. *Научни циљ*

Научни циљ овог рада јесте демонстрирање оправданости конвергенције два (хипотетички) одвојена концепта у ревизији информационих технологија – условно именованих као финансијски оријентисани – традиционални и технолошки

оријентисани – савремени. Циљ је утврђивање саме оправданости овакве поделе, затим утврђивање главних карактеристика сваког од ових концепата – основних појмова, терминологије (именског простора), методологије, дакле њихове таксономије, и на крају идентификовање могуће парцијалне или укупне интеграције – спајањем комплементарних области или усклађивањем међусобно конфликтних сегмената.

1.4.2. Конкретни циљ

Овај рад такође тежи да својом структуром и садржајем у што већој мери одговори препознатој потреби за основном стручном литературом у области ревизије ИТ код нас. Циљ рада је да се на једном месту пружи свеобухватан преглед теоријских аспеката заједно са практичним и искуством стеченим знањима неопходним за успешан професионални рад у овој уско-стручној области.

1.5. ТОК ИСТРАЖИВАЧКОГ ПРОЦЕСА И МЕТОДИ ИСТРАЖИВАЊА

1.5.1. Ток истраживачког процеса

Истраживачки процес чине две целине: истраживање и презентација резултата истраживања. Истраживање је текло у четири фазе: постављање проблема, формулисање хипотезе, проверавање хипотезе и потврђивање (верификација) хипотезе. Презентација резултата је у форми писаног рада, са структуром која прати утврђене стандарде за радове овог типа и садржајем који одражава ток и резултате истраживања. Практични део рада је издвојен у посебну целину – студију случаја. Такође, рад је пропраћен одговарајућом визуелном презентацијом – серијом слајдова са сажетим приказом читавог истраживачког рада и његових резултата.

1.5.2. Основни научни методи

При дефинисању проблема и постављању хипотетичког оквира, коришћене су информације прикупљене емпиријски у току вишегодишњег практичног рада. Упоредо, примењена је метода истраживања литературних података из расположивих штампаних публикација и *on-line* извора (Интернет). На овако прикупљеним информацијама примењени су методи селекције, елиминације и синтезе. За проверу и потврђивање хипотезе коришћени су методи упоредне анализе, генерализације и аналитичке дескрипције. У студији случаја, ради практичне потврде изведених закључака, коришћен је и експериментални метод.

1.5.3. Логички методи

У свим фазама истраживачког рада коришћени су формално-логички методи дедукције и индукције, упоредо са неформално-логичким методима емпиријске опсервације, компарације, критичког мишљења и когнитивног просуђивања.

1.5.4. Статистички методи

У овом раду статистички методи нису коришћени, што је последица специфичности конкретног хипотетичког оквира и циљева истраживања.

2. РЕВИЗИЈА ИНФОРМАЦИОНИХ ТЕХНОЛОГИЈА

2.1. УВОД

Дефинитивни консензус око улоге и одговорности ревизије информационих технологија још увек није постигнут. Стручна јавност и професионална теорија и пракса данас нуде различите дефиниције, радне оквири и приступе овој области. Сведоци смо ситуације у којој не само да се користе различити називи за исте и врло сличне појмове (ревизија информационих технологија, ревизија информационих система итд) већ се иза истог назива крију сасвим различити, па чак и међусобно супростављени концепти.

Ревизори информационих технологија често су схваћени само као техничка подршка финансијским ревизорима, неко ко једноставно оперише информатичким средствима искључиво по налогу и на захтев конвенционалне ревизије. Тако схваћен, технолошки ревизор је неко ко рукује подацима, генерише упите према базама података и добијене табеле „слаже” у одговарајуће извештаје. Супротно називу који носи, овакав приступ управо онемогућава праву технолошку ревизију и чини да главни ризици које организацији доноси примена информационих технологија остану потпуно неоткривени.

Друго, савременије, схватање је да се технолошки ревизори баве тзв контролама у информационим системима. Ове контроле су заправо управљачко-контролни механизми који постоје у информационим системима ради тога да се управи (менаџменту) омогући примена стандардних мера управљања и контроле и у дигиталном домену. Контроле у ИС се обично деле на опште (генералне) и апликативне контроле. Генералне контроле су уграђене у опште информатичке процесе и сервисе (на пример развој система, управљање променама, безбедност, организациона структура ИС/ИТ), док се апликативне контроле везују за имплементацију пословне логике у информационим системима (на пример тачност, целовитост и валидност података, аутентификација, ауторизација, раздвајање дужности итд). Иако овакво схватање даје технолошком ревизору знатно ширу и значајнију улогу, бавећи се искључиво контролама у ИС он остаје и даље изолован од већег дела информационих технологија и без могућности да обавља целовиту технолошку ревизију.

Један начин којем се прибегава у циљу превазилажења постојања области непокривених ревизијом јесте увођење низа врло уско специјализованих ревизорских функција. Ревизија безбедности, ревизија усклађености, ревизија против преваре, итд, само су неки од примера. Као по правилу, већина ових активности обавља се потпуно независно од остатка технолошке ревизије. Због тога, иако омогућавају да се предметна област истражи „у дубину”, овакви концепти нужно пате од међусобне неповезаности и често испољавају неку врсту аутизма у односу на целину проблематике информационих технологија.

По свом исходишту, еволуцији и правцу развоја, савремени погледи на ревизију информационих технологија могу се груписати у две главне групе. Једна је настала у контексту традиционалне ревизије, док се друга развила у окружењу информационих технологија. Условно, у контексту овог рада, можемо их назвати традиционална

(финансијски оријентисана) ревизија информационих технологија и савремена (информатички оријентисана) ревизија информационих технологија.

а) Ревизија информационих технологија настала у контексту традиционалне (или конвенционалне) ревизије.

Изворно, ревизија је активност уско усмерена на утврђивање исправности рачуноводствених исказа, односно финансијских извештаја неке организације. Традиционална ревизија постоји у два облика – екстерна (спољашња, вањска) и интерна (унутрашња) ревизија. При томе је екстерна ревизија углавном фокусирана на област финансија, због чега се често назива и финансијска ревизија, и има за циљ давање објективног и независно стеченог мишљења о исправности финансијских исказа (извештаја) неког правног лица (компаније, јавне или државне установе итд), што се углавном односи на релевантност, тачност и целовитост предметних финансијских извештаја. За разлику од екстерне, интерна ревизија се креће у знатно ширим оквирима и окреће се свим проблемима који генерално могу да спрече одређену организацију у постизању њених циљева. Интерна ревизија систематски и методично преиспитује системе интерних контрола у предметној организацији и анализира све пословне процесе и процедуре са циљем да открије проблеме, укаже на њих и да препоручи одговарајуће мере. Док екстерну ревизију у некој организацији обављају засебне, специјализоване и за то овлашћене фирме, интерна ревизија се по правилу налази унутар саме организације чију ревизију врши и представља њен саставни део.

Са развојем информационих технологија, дошло је до њихове масовне примене у свим пословним системима. Сви пословни процеси, укључујући и финансије, притом добијају своју имплементацију у одговарајућим информационим системима, чиме се успоставља трајна и врло дубока зависност целокупног савременог света од информационих технологија. Све врсте бизниса, финансијске институције, државне администрације, системи управе, медији и све остале организације зависе у огромној мери од информационих технологија које користе.

Природно, у овако насталим условима, ревизија (пре свега интерна) временом бива принуђена да се бави и технологијом. Развија се посебна активност унутар ревизије која је само томе посвећена. Она најпре креће да анализу пословних процеса прилагоди новим условима па утврђује начине за анализу одговарајуће апликативне логике преко које су ти пословни процеси имплементирани у информационим системима. Даље, ревизија почиње да тражи логику традиционалних система интерних контрола унутар информационих система и да проналази начине да се у оквиру тих контрола открију слабости и практичне могућности за њихово превазилажење.

Овај правац развоја је данас доспео до тачке у којој ревизија информационих технологија почиње да бива препозната као засебна дисциплина у оквиру конвенционалне интерне ревизије. Могу се издвојити следеће карактеристике овако успостављене ревизије информационих технологија:

- Ревизори се бирају већином из редова стручњака за рачуноводство и финансије који се додатно образују за информатичку област. Стручњаци техничког профила су у мањини и махом чине само тзв „информатичку подршку” ревизорима
- У већини случајева, фокус је углавном унутар две групе контрола: прво, тзв

генералних компјутерских контрола и, затим, контрола у оквиру апликација. Предмет ревизије је ограничен углавном на оне елементе информационих система који се могу схватити као дигитална аналогија одговарајућих конвенционалних механизма контроле: аутентификација, ауторизација, потврђивање трансакција, валидација уноса података, валидација приказа података, раздвајање (сегрегација) дужности и слично. У већини случајева, фокус остаје затворен унутар апликативног слоја.

- Ревизија је углавном интерна. Независност и објективност у односу на друге делове организације се притом постижу успостављањем засебне специјализоване целине унутар организационе структуре, што није увек могуће и доста често и није случај.
- Постоје предуслови за развој формалног и процедуралног приступа ревизији, па чак и одређени притисци унутар законске и професионалне регулативе за кретање у том смеру; у исто време, слобода избора је мања, најчешће нема истраживачког и експерименталног рада, скуп коришћених алата је врло ограничен.
- Фаворизовани су ревизорски приступи који полазе од организационе шеме, од поделе улога и одговорности у организацији а у новије време и од претходно процењеног ризика; супротно томе, приступи који узимају за полазиште тополошке, функционалне и друге сложеније технолошке карактеристике система ретко се или уопште не користе.

б) Ревизија информационих технологија настала у контексту самих информационих технологија.

Овај правац развоја је текао потпуно независно од конвенционалне ревизије и без икакве везе са професијом традиционалног ревизора. Он је настао као саставни део самих информационих технологија и то као исказ природне потребе да се технологија сама по себи мора подвргавати ревизији у току целог свог животног циклуса. Развој технологија и техничких решења која се на њима заснивају одувек је подразумевао и потребу за ревизијом. Све фазе животног циклуса једног ИТ решења обавезно укључују детекцију, реакцију и корекцију, па је тако, у овом контексту, на природан начин дошло до препознавања потребе да се ревизија информационих технологија издвоји у посебну дисциплину у оквиру информатике и да буде прихваћена као засебна професија. Овако схваћена ревизија информационих технологија има следеће карактеристике:

- Ревизори су углавном техничког стручног профила – рачунарство, информатика, телекомуникације и сл; додатна едукација из области економије, финансија, рачуноводства, менаџмента итд врло се ретко или уопште не спроводи.
- Предмет ревизије је технологија у целини а не само поједини делови система или изоловане апликације; присутна је склоност да се технологија посматра као искључиви предмет ревизије, при чему се традиционални предмети ревизије – финансијски, рачуноводствени итд – често потпуно изузимају из разматрања.
- Ревизор је позициониран изван организације која је предмет ревизије – технологије су у приватном власништву клијента ревизије или добављача/произвођача, те је ревизор најчешће у позицији да нема сукоба интереса.
- Постоје изразити предуслови за независност и објективност у раду, као и за истраживачки и експериментални приступ.
- Постоји већа слобода у избору поступака, техника и алата, али се често заостаје у формализацији поступака, документовању и процедуралном приступу ревизији.
- Приступи који подразумевају дубље познавање технологије се овде не запостављају, што је природно с обзиром на контекст који је по себи доминантно

технички; напротив, топологија, функционална подела, вишеслојност система и слично овде су знатно присутнији него у традиционално схваћеној ревизији; у новије време, поред стриктно технолошких, у први план доспевају персонални аспекти, социјални инжињеринг, етичко хаковање и друге, често врло инвентивне, технике ревизорског приступа.

2.2. ОСНОВНИ ПОЈМОВИ – МЕСТО И УЛОГА РЕВИЗИЈЕ

2.2.1. Дефиниција интерне ревизије

Данас постоји високи степен сагласности око појма интерне ревизије – стручни кругови се углавном придржавају дефиниције коју је развио Институт интерних ревизора (*The Institute of Internal Auditors – IIA*). Према овој дефиницији, интерна ревизија је независна и објективна активност која даје савете и пружа уверења са циљем да увећа вредност и унапреди делатност једне организације. Она помаже организацији у постизању њених циљева тако што систематичним и дисциплинованим приступом евалуира (процењује) и унапређује процесе управљања ризиком, контроле и управљања организацијом.

Према општеприхваћеној интерпретацији ове дефиниције, интерна ревизија је усмерена на сваку претњу која угрожава или би могла да угрози реализацију пословних циљева организације за коју ради. Интерна ревизија делује превентивно, детективно и корективно. Превентивно деловање се огледа у саветодавној функцији интерне ревизије, кроз коју се организацији дају препоруке како да избегне излагање најзначајнијим ризицима пре него што се они појаве. Детективно деловање се састоји у откривању слабости и изложености реалним ризицима, и пружању уверења о стању у којем се организација налази у погледу тих ризика. На крају, корективно деловање се огледа кроз систем објективног извештавања у којем се руководству организације препоручују конкретне мере за унапређење и отклањање свих откривених сметњи које ометају организацију у испуњењу њених циљева.

Ова дефиниција је резултат вишегодишњег настојања да се у што сажетијој форми изразе суштина, основне карактеристике и циљеви професије интерног ревизора. У Прилогу 4.1 дата је табела са историјским прегледом најзначајнијих дефиниција појма интерне ревизије, као својеврсна илустрација њеног еволутивног развоја. Дефиниције су дате без превода, у изворном облику, преузетом из првог издања књиге *The Internal Auditing Handbook* (K.H.Spencer Pickett)[29].

У свим дефиницијама се наводе карактеристике независности и објективности. Без ове две карактеристике интерна ревизија не може да егзистира. То су њени основни принципи и претпоставке – они одражавају суштину и основну мотивацију њене егзистенције.

2.2.2. Независност и објективност интерне ревизије

Принципи независности и објективности представљају темељ интерне ревизије као професије.

Међународни стандарди за професионалну праксу интерне ревизије (*International*

Standards for the Professional Practice of Internal Auditing) [33] које је објавио Институт интерних ревизора (*The Institute of Internal Auditors – IIA*) успостављају појмове организационе и индивидуалне независности и објективности интерног ревизора у Стандарду 1100. Стандард 1100 дефинише независност и интерпретира је као „ослобођеност од околности које би могле да угрозе непристрасност интерне ревизије или њиховог руководиоца у спровођењу активности за које су одговорни”. У том циљу, стандард прописује да руководилац интерне ревизије мора имати могућност директног приступа највишем руководству и Одбору директора организације којој припада.

Даље, Стандард 1100 каже да је објективност „непристрасан ментални став који ревизорима омогућава да узму учешће у својим активностима са пуном вером у своје резултате и без компромиса у погледу квалитета”. Објективност подразумева да ревизор „неће дозволити да његово просуђивање о питањима ревизије буде потчињено било чијем утицају, независно од формалне субординације у коју је укључен”.

Посебне секције у Стандарду 1100 третирају организациону независност (1110), индивидуалну објективност (1120), као и обавезу разоткривања сваке сметње у погледу независности и објективности (1130).

Организациона независност се постиже тако што руководилац интерне ревизије директно одговара највишем нивоу управе у организацији. То је, по правилу, Одбор директора (управни одбор, извршни одбор или одговарајући врховни орган управе у датој организацији). Линија његове одговорности мора бити ослобођена утицаја било које организационе целине која би се могла наћи у улози клијента ревизије. Другим речима, интерна ревизија не сме да буде у положају субординације у односу на било коју пословну функцију која је предмет ревизије.

Индивидуална објективност огледа се у томе што интерни ревизор мора да буде непристрасан, не сме да буде подложен утицајима са стране и мора да буде ослобођен сваког сукоба интереса. Стандард посебно разматра сукоб интереса као ситуацију у којој ревизор којем је поверен ревизорски задатак поседује лични или професионални интерес супростављен циљевима постављеног задатка у мери која утиче или би могла утицати на крајњи резултат. Према Стандарду 1120, сукоб интереса може постојати чак и у случају да ревизор не почини никакав неморалан или нелегалан акт – довољна мера за утврђивање сукоба интереса је већ и само постојање могућности да се посумња или изгуби поверење у ревизора лично, у ревизорску активност у којој је узео учешће или у професију у целини.

Овако стриктно санкционисање индивидуалне објективности додатно је учвршћено обавезом да се свака могућа сметња која би могла да угрози објективност и независност интерне ревизије или интерног ревизора мора пријавити и ставити на знање свим странама укљученим у предметну ревизорску активност и на које би резултат предметне ревизорске активности могао имати утицај. Према томе, сваки лични конфликт, сукоб интереса, недоступност информација, сваки недостатак потребних ресурса и слично, морају бити на време пријављени и обелодањени пре него што учине утицај на резултате ревизије.

2.2.3. Професионална етика

Професија интерног ревизора се поставља у чврст и јасан етички оквир, формулисан кроз професионални етички кодекс. Свака организација је у обавези да своје интерне ревизоре веже за један такав кодекс.

Етичким кодексом једне организације промовише се етичка култура у професији интерне ревизије. Њиме се успостављају принципи који су релевантни за професију и професионалну праксу интерне ревизије и дају правила понашања која нормирају очекивано понашање интерног ревизора у његовом раду. Ова правила помажу у практичној примени принципа и служе као упутство интерним ревизорима за етички исправне поступке.

Иако у општем случају ови кодекси могу бити различити и по садржају прилагођени потребама индивидуалних организација, они генерално морају бити усклађени са основним принципима професионалне етике које је успоставио Институт интерних ревизора (IIA) у свом Етичком кодексу (*The Institute of Internal Auditors Code of Ethics*) [34].

Основни принципи којих се интерни ревизори морају придржавати су интегритет, објективност, поверљивост и компетентност.

Принцип интегритета:

Својим поступцима интерни ревизори исказују лично поштење, одговорност и доследно поштовање закона и етичких норми, чиме заслужују одговарајуће поверење, што чини основу за свако даље ослањање на њихове процене.

Принцип објективности:

Интерни ревизори исказују највишу могућу меру професионалне објективности приликом прикупљања информација, њихове евалуације и извештавања о процесима и активностима који су предмет њиховог испитивања. Интерни ревизори дају избалансиране процене свих релевантних околности и не падају под утицај других или личних интереса приликом формирања својих закључака.

Принцип поверљивости:

Интерни ревизори поштују вредност и власништво информација које добију и не разоткривају их без одговарајућег овлашћења осим ако не постоји правна или професионална обавеза да то учине.

Принцип компетентности:

Интерни ревизори примењују сво знање, вештине и искуство неопходно за вршење интерне ревизије.

Етички кодекс прописује и правила понашања интерног ревизора, која даје у облику обавезујућих одредби, и то за сваки од принципа понаособ.

У циљу поштовања принципа интегритета, интерни ревизори се обавезују:

- да ће обављати свој рад поштено, вредно, пажљиво и одговорно

- да ће поштовати закон и разоткривати незаконите и непрофесионалне поступке
- да неће бити укључени у било какве илегалне активности, као и активности које вређају професионални углед интерне ревизије или углед организације којој припадају
- да ће поштовати и давати допринос законитим и моралним циљевима организације

У циљу поштовања принципа објективности, интерни ревизори се обавезују:

- да неће учествовати ни у каквој активности која би могла да утиче, или се за њу сматра да би могла да утиче на непристрасност у оценама
- да неће прихватити ништа што би могло да утиче или се сматра да би могло да утиче на непристрасност у оценама
- да ће разоткривати сваки материјал који би, у случају да остане сакривен, могао да утиче на садржај ревизорског извештаја

У циљу поштовања принципа поверљивости, интерни ревизори се обавезују:

- да ће бити савесни у коришћењу и заштити информација до којих су дошли вршећи своје дужности
- да неће користити информације за личну добит или на начин који би био у супротности са законом или штетан по пословне интересе организације

У циљу поштовања принципа компетентности, интерни ревизори се обавезују:

- да ће узимати учешћа само у оним активностима за које поседују неопходна знања, вештине и искуство
- да ће у свом раду поштовати професионалне стандарде и најбољу препознату професионалну праксу у области интерне ревизије
- да ће непрекидно радити на усавршавању својих знања и вештина, као и ефективности и квалитета вршења интерне ревизије

За интерне ревизоре, свако кршење етичког кодекса подлеже евалуацији и третману према одговарајућим дисциплинским процедурама пословне функције и организационе целине којој интерни ревизор припада. Чињеница да одређени поступак није директно поменут у етичком кодексу не представља сметњу за оцену његове прихватљивости односно неприхватљивости нити умањује одговорност интерног ревизора за такав поступак.

2.2.4. Место и улога интерне ревизије

Професија интерне ревизије бележи константан развој од времена Другог светског рата до данас. Овај развој текао је паралелно са напретком теорије и праксе менаџмента, којим је делимично био и условљен. Иако постоје извесне концептуалне сличности са финансијском ревизијом, контролом квалитета или контролом усклађености са законима и регулативом (*Compliance*), са којима има умногоме и заједничке теоријске основе, интерна ревизија је пронашла своје место и улогу у савременим пословним процесима. Према савременој дефиницији, интерна ревизија има веома широко поље деловања. Она помаже организацији у постизању њених циљева, тако што се усредсређује на евалуацију и унапређивање процеса управљања ризиком, свих врста интерних контрола и процеса управљања организацијом. То значи да интерна ревизија

има улогу да открије и процени све оно што би могло једну организацију да омете у реализацији њених циљева и да пружи препоруке мера за отклањање тих сметњи.

Већ је речено да се, у циљу постизања потребног нивоа независности, интерна ревизија организационо поставља тако да одговара директно највишој управи у организацији. Међу организацијама постоје велике разлике не само у погледу назива органа највише управе, већ и у погледу тога како је највиша управа уређена, каква су њена овлашћења и одговорности. Премда постоји и могућност да орган највише управе чини један човек, најчешће је то колективно тело, чији чланови се бирају директно од стране власника или гласањем. Општи назив за такво тело је Одбор (*Board*). У међународној пракси се срећу многи називи (*board of directors, board of trustees, board of governors, board of managers, executive board*), док је код нас најчешћи назив за такво тело „управни одбор”.

Управни одбор по правилу успоставља једно засебно тело (пододбор), којем се поверавају сва овлашћења везана за питања интерне ревизије. По својој улози, то тело је „наручилац” послова интерне ревизије – на њему се технички завршава линија одговорности интерне ревизије. Оно усваја годишње планове рада интерне ревизије, њему се подносе ревизорски извештаји које оно анализира и о којима затим реферише Управном одбору. То тело је једина инстанца у организацији која је овлашћена да смени (или да постави) руководиоца интерне ревизије. Изворни назив за овај орган управе је „одбор за ревизију” (*Audit Committee*), али у домаћој пракси уместо речи „одбор” често срећемо и „комитет”, „комисија” и слично. Чланови одбора за ревизију не могу бити извршни директори из састава предметне организације, јер би у противном био прекршен принцип организационе независности интерне ревизије.

Према томе, директна одговорност интерне ревизије управном одбору технички се реализује преко одбора за ревизију, као специјализованог пододбора. У том органу управе је концентрисана „сва власт” коју једна организација има или може имати над интерном ревизијом.

У пракси постоје примери који одступају од овог правила. У мањим организацијама, у организацијама где нема управних одбора, или тамо где постоје друге организационе специфичности, интерна ревизија може бити постављена тако да одговара директно генералном директору. Такође, постоје и организације које имају управни одбор без одбора за ревизију, итд.

Према томе, место интерне ревизије у организационој шеми може бити различито, зависно од типа, величине или других карактеристика саме организације. Једини критеријум по којем се може утврдити да ли је то место одговарајуће јесте да ли то место омогућава несметано испуњење улоге интерне ревизије и остваривање њених циљева на независан и објективан начин.

2.3. МЕСТО И УЛОГА ТЕХНОЛОШКЕ РЕВИЗИЈЕ

2.3.1. Настајак и историја технолошке ревизије

У оквиру интерне ревизије, први облици технолошке ревизије јавили су се под називом ревизија електронске обраде података (ревизија ЕОП), у време када су почели да се

уводе први рачунари у рачуноводствене системе. Сматра се да је први такав систем уведен у америчкој компанији Генерал Електрик (*General Electric*) 1954. године. Све до средине шездесетих година прошлог века ревизори су се у послове ревизије ЕОП упуштали врло ретко и у малом броју организација. Међутим, средином шездесетих, са појавом мањих и јефтинијих рачунарских система, долази до одговарајућих промена и у овој области. Појава све већег броја различитих система за рачуноводство доводи до покретања иницијативе у водећим ревизорским кућама за утврђивање општих принципа и правила по којима ће се одвијати ревизија ЕОП. Године 1968, Амерички институт сертифицираних јавних рачуновођа (*AICPA – American Institute of Certified Public Accountants*) објављује први приручник за ревизију АОП (*Auditing & EDP*). У исто време, појављују се и први софтверски алати за аутоматизовану ревизију.

Убрзо, формира се прво струковно удружење ревизора ЕОП (*EDPAA – Electronic Data Processing Auditors Association*). Ово удружење 1977. године издаје прву верзију „Контролно – управљачких смерница” (*Control Objectives*), које су биле претеча данашњег оквира КОБИТ (*COBIT – Control Objectives for Information and Related Technologies*). ЕДПАА мења свој назив 1994. године у *ISACA – Information Systems Audit and Control Association*.

Од почетка седамдесетих, технологија микрорачунара је постепено истиснула велике рачунарске системе са тржишта и експанзија информационих система базираних на тим технологијама је од тада до данас непрестано убрзавала. Упоредо са тим процесом, развијају се и теорија и пракса технолошке ревизије.

У исто време, у оквиру саме информатике, препозната је потреба да се читав животни циклус развоја информационих система прати одговарајућим ревизорским активностима. Планирање, пројектовање и развој система прате се одговарајућим контролама – квалитет, безбедност, ефективност и ефикасност система подвргавају се сталним проверама и оцењивању како би се обезбедила конкурентност на тржишту технолошких решења. Такође, у области примене и коришћења технологија, уводе се системи за контролу како би се избегли или умањили ризици од погрешне имплементације, конфигурације, неадекватног одржавања или корисничких грешака. Све ово је временом конвергирало, тако да данас имамо успостављену засебну теорију и праксу технолошке ревизије у области информационих технологија и система.

2.3.2. Дефиниција технолошке ревизије

Иако се око дефиниције, места и улоге опште ревизије (интерне и екстерне) успоставио високи степен сагласности у стручним круговима, то се, нажалост, не може рећи и за специјализовану ревизију савремених технологија и технолошких система. Као што је и раније поменуто, већ око самог назива постићи неусаглашеност. Данас се најчешће користе називи „ревизија информационих система” и (нешто ређе) „ревизија информационих технологија”, међутим значења нису усаглашена и често се у значајној мери разликују. У различитим контекстима, исти назив може бити коришћен у различитим значењима. Такође, у неким контекстима, ова два назива се третирају као синоними и користе се да означе исти појам.

Већина извора (видети: *7.Референце и литература*) уопште не наводи никакву дефиницију технолошке ревизије, без обзира на то који назив користе. Углавном, аутори ревизију технологија виде као додатак или надоградњу на већ формирану и добро

познату целину интерне ревизије. У неким изворима ([4], [12], [20], [29], [30], [31] и [33]), централна тема је интерна ревизија са својом традиционалном оријентацијом на финансијске извештаје и припадајуће пословне процесе. У њима се технологије и технолошки системи третирају једноставно као савремена средства за вођење послова и у којима морају бити имплементирани одређене контролне – управљачке мере у циљу контроле пословних ризика. Међутим, ризици који потичу непосредно од самих технологија које се користе, ризици који долазе од њихове примене, ризици у процесима управљања тим технологијама, њихове слабости и контролне – управљачки механизми за превазилажење тих слабости се или уопште не разматрају или се једва помињу. Неки извори препознају специфичности технолошких ризика и одговарајућих контролних – управљачких мера (на пример [9], [26]) и улазе у детаље ревизорских поступака, техника или алата који се користе у том домену, али се општи став или закључак о улози и месту технолошке ревизије ни ту не даје јасно и прецизно. Углавном, могу се наћи извори о томе „како” се врши технолошка ревизија, док се ретко наилази на разматрања о томе „шта” технолошка ревизија треба да ради. Читалац је приморан да формира сопствену представу о циљевима, делокругу, месту и улози технолошке ревизије индуктивним путем.

Најближе покушају да се пружи дефиниција технолошке ревизије дошао је Џагдиш Патак (*Jagdish Pathak*) у својој књизи *Information Technology Auditing: An Evolving Agenda* [26], иако није експлицитно поменуо да се ради о дефиницији.

Тај став гласи овако:

„Ревизија информационих технологија је процес прикупљања и процене (евалуирања) доказа о томе да ли један информациони систем:

- штити средства и имовину,
- одржава интегритет података,
- ефективно достиже циљеве које је поставила организација и
- ефикасно користи ресурсе.”

Иако успева да пренесе интуитивно исправну представу о томе шта заправо технолошка ревизија представља, овај став ипак не представља довољно добру дефиницију и проблематичан је по основу неколико критеријума. Детаљније разматрање проблема који се јављају при покушају дефинисања технолошке ревизије даје се у тачки 4. (*Дискусија*), заједно са другим отвореним питањима полемичког или дискутабилног карактера на које указује овај рад.

2.3.3. Место технолошке ревизије у организацији и линија одговорности

Улога технолошке ревизије, квалитет њеног учинка и степен независности у највећој мери су условљени организационим положајем и линијом њене непосредне одговорности. У пракси се срећу различита решења, зависно од типа организације, њене величине или делатности којом се бави.

а) Технолошка ревизија као део функције интерне ревизије

Технолошка ревизија се најчешће позиционира унутар организационе целине за интерну

ревизију, и то на два могућа начина. Први начин је да се за технолошку ревизију унутар интерне ревизије оформи посебан сектор (служба, одељење), што је применљиво у већим организацијама, где је интерна ревизија бројнија и где постоје услови за тако нешто. Други начин је да се технолошки ревизори „измешају” са осталима, без формирања засебне организационе целине. То је применљиво у мањим организацијама, где је интерна ревизија малобројна и где се захтева таква (тзв „равна”) организација.

Овде је у оба случаја положај технолошке ревизије директно условљен положајем саме интерне ревизије. Уколико је целина интерне ревизије позиционирана тако да су испуњени услови за њену организациону независност, онда је овакав организациони положај за технолошку ревизију вероватно и најповољнији са становишта ефикасног испуњења њене улоге, видљивости и утицаја у организацији.

б) Технолошка ревизија као део функције за технику/технологије (ИТ, ИКТ)

Ово решење се нешто ређе примењује, али је релативно често у организацијама чија је пословна делатност претежно технички или технолошки оријентисана. У таквим организацијама је чест случај да организационе целине за технику или технологију имају доминантан положај. Исто тако, зависност савременог пословања од информационих технологија је понекад толико велика да су чести примери „експанзионизма” информационих технологија чак и у компанијама чији послови нису техничко – технолошког карактера. У сваком случају, у пракси срећемо организације у којима руководиоци информационих технологија имају посебно велику (формалну и неформалну) моћ па им је омогућено да, колоквијално речено, „имају свог ревизора”.

Веома слично стање је и у неким доминантно финансијским установама (банке, осигурања, берзе, инвестициони фондови и сл), само што се тамо моћ концентрише у рукама финансијских директора. Тамо је честа ситуација да читава (па тако и технолошка) ревизија буде директно подређена финансијском директору.

Оваква решења понекад могу да буду врло практична и функционална, посебно када су доминантни положај и моћ у организацији озваничени и формализовани. На пример, када директор ИТ (или финансија) има истовремено положај подпредседника компаније или је члан управног одбора („борда” директора), онда то ревизији може да обезбеди високу видљивост и велики значај у организацији.

Међутим, оваква решења имају принципијелно значајне недостатке. Пре свега, у погледу организационе независности јер су ревизори доведени у ситуацију да буду део организационе целине која истовремено треба да буде и њихов најважнији клијент. Јасно је да постоји озбиљан сукоб интереса између ревизорске функције и функције којој ревизори организационо припадају. Према томе, чак и када ревизија одлично функционише у односу на остатак организације, остаје озбиљан и трајан проблем функционисања у односу на целину којој она припада и чијем руководиоцу је непосредно подређена.

в) Технолошка ревизија као део функције корпоративне или ИТ безбедности

У неким организацијама пословна филозофија и култура су такве да се технолошка ревизија схвата веома уско – пре свега или чак искључиво као ревизија безбедности у

компанији. То је посебно чест случај у компанијама које се баве производњом или услугама у домену безбедности (смарт и СИМ картице, шифарски системи, ИТ заштита итд). Ту онда често срећемо организациона решења у којима се технолошка ревизија смешта унутар организационе целине задужене за безбедност. Зависно од организационих специфичности, то може бити посебно информатичка безбедност или, што је чест случај у новије време, целокупна корпоративна безбедност, где су организационо уједињене технолошка и физичка (физичко – техничка, противпровална, противпожарна и друга) заштита. Постоје и друге варијанте овог решења, где се технолошка ревизија или ревизија безбедности организационо везује за одељење за управљање ризиком и други слични примери.

Без обзира на укупну ефикасност и успешност коју овако постављена технолошка ревизија може да има у датој организацији, у погледу независности и сукоба пословних интереса остају исте примедбе као и у претходном случају.

г) **Екстерна технолошка ревизија**

Многе организације немају сопствену технолошку ревизију. Разлози за то могу бити различити. Пре свега, код великог броја малих и средњих организација нема економског оправдања за успостављање сопствене ревизорске функције (посебно технолошке). Неке организације, иако довољно велике и економски снажне, не желе да имају сопствену технолошку ревизију и сматрају да је коришћење екстерних услуга (тзв „*outsourcing*”) за њих економичније решење. На крају немали број организација уопште и не препознаје потребу за сталним процесима ревизије, већ своје системе подвргавају ревизији само онда када за то постоји обавеза или се појави неки други разлог. Уз све то, није без значаја ни фактор окружења у којем организација ради, као што су услови на локалним тржиштима квалификоване радне снаге, који отежавају или онемогућавају формирање интерне ревизорске функције чак и онда када организација то настоји да учини.

Технолошка ревизија је релативно нова стручна област, број квалификованих стручњака је још увек сразмерно мали, поготово у мањим земљама, тако да је у таквим окружењима веома тешко засновати и одржати сопствену технолошку ревизију. Ово са друге стране погодује глобализацији тржишта, тако да данас велики број компанија нуди услуге технолошке ревизије клијентима широм света. С обзиром на то да је реч о ревизији информационих и комуникационих технологија, код којих је многе операције могуће обавити „на даљину”, а то значи и без претерано великих трошкова, то пружа прилику чак и веома малим стручним тимовима да воде послове на глобалном нивоу. Може се рећи да је ревизија информационих и комуникационих технологија једна од ретких области глобалног пословања у којима веома мале компаније могу да буду врло конкурентне великим или чак супериорне у односу на њих.

У новије време уочава се тренд суб-специјализације у оквиру ове врсте услуга. Појављују се посебне (веома уско специјализоване) услуге, као што су ревизија информатичке безбедности (*Information Security Auditing*), тестирање на пробој (*Penetration Testing*), услуге управљања и контроле система безбедности (*Managed Security Services*), ревизија изворног кода апликативног софтвера (*Source Code Auditing*), дигитална форензика (*Digital Forensics*) итд.

У Србији је тржиште услуга технолошке ревизије веома неразвијено, не само у погледу

понуде (мали обим и низак квалитет) већ и погледу потражње. Веома мали број привредних субјеката уопште препознаје потребу за овом врстом услуга, тако да су малобројни клијенти углавном упућени на понуђаче са стране.

2.3.4. Специфична независност и објективност технолошке ревизије

Технолошка ревизија у погледу независности и објективности има неколико специфичности које заслужују додатно разматрање.

а) Интерна технолошка ревизија

Обично се сматра да је довољно обезбедити организациону независност ревизије у целини, па да ће тиме бити испуњени и сви предуслови за независност технолошке ревизије. Међутим, у многим организацијама то уопште није тако.

Као прво, веома честа је финансијска (буџетска) зависност од клијента технолошке ревизије.

Традиционална (финансијска) интерна ревизија користи минимум информационих технологија. Информатичка опрема једног ревизора не одступа много од опреме типичног канцеларијског радника: радна станица опремљена канцеларијским софтвером, уобичајени пословни софтвер, клијенти за електронску пошту и Интернет. Због тога одељења интерне ревизије у већини организација немају засебан буџет за информатичка средства већ се информатички опремају из централног буџета

Међутим, технолошка ревизија има знатно веће и веома специфичне информатичке потребе. У погледу софтвера, постоји потреба за низом врло специфичних алата, од којих неки раде на специфичним оперативним системима, неки су веома скупи или захтевају врло специфичне услове лиценцирања итд. У погледу потребног хардвера, радно место технолошког ревизора такође одступа од уобичајеног. Поред стандардне канцеларијске радне станице, постоји потреба за додатним рачунарима на којима ће се покретати специјализовани ревизорски поступци (за сваки оперативни систем посебно), тестирати ревизорски налази, испитивати нове технике, алати итд. Неки од ових додатних рачунара морају да буду преносиви (*laptop, netbook, PDA, smart phone*), што такође одступа од стандарда за типично радно место.

У већини организација, целокупна информатизација (па и одговарајући буџет) је под контролом засебне организационе целине – дирекције (сектора, одељења, службе) за информационе технологије. Према томе, технолошка ревизија у таквим организацијама налази се у положају директне зависности од свог главног клијента ревизије. Клијент ревизије је у позицији да директно утиче на опремљеност, услове за рад, па самим тим и на одвијање процеса технолошке ревизије и њихову успешност. Ово не само да је супротно основним принципима ревизије већ у многим случајевима представља нерешиви проблем који може да доведе до потпуне блокаде рада интерне технолошке ревизије.

Поред буџетске зависности, технолошка ревизија се врло често налази и у условима непосредне технолошке зависности од свог клијента. Пре свега, радно место технолошког ревизора подразумева специфичну ауторизацију за приступ

информацијама и технолошким ресурсима. У идеалном случају, права за приступ систему требало би да задовоље два основна принципа: принцип минималних овлашћења, по којем се кориснику дају овлашћења не већа од оних која су довољна за обављање његовог посла (*Least Priviledge*) и принцип неопходне информисаности, по којем се кориснику дају на располагање све информације које су му потребне за обављање његовог посла (*Need to Know*). Примена ових принципа на корисника који ради на радном месту ревизора за ИКТ представља веома велики практичан проблем. Такав корисник би требало да има приступ до (апсолутно) свих информација у систему, али без права њихове модификације (писања или брисања). Треба имати у виду да се ово односи на приступ свим технолошким средствима – серверима, радним станицама, мрежи и мрежној опреми, оперативним системима, базама података, апликацијама итд. У сложеним системима овако нешто је веома тешко, ако не и немогуће за реализацију. Зато неки стандарди и препоруке (на пример *ISF – Information Security Forum*) предлажу једноставно решење по којем се технолошким ревизорима додељују највиша права приступа у систему; у случају оперативног система *Windows* и примењене *Active Directory* технологије то би, на пример, значило да ревизори треба да буду учлањени у групу администратора домена, без икаквих ограничења у погледу приступа. Очигледно, Форум је закључио да је принцип независности значајнији од принципа минималних овлашћења, па је овај други, у немогућности идеалног решења, жртвовао у корист првог.

Поред тога, у погледу конфигурације радних станица, локалне мреже и мрежних уређаја, за технолошке ревизоре је потребно омогућити низ изузетака у односу на типичне корпоративне политике: филтрирање саобраћаја, дозвољене протоколе и сервисе, слободу промене ИП адреса итд.

Непотребно је наглашавати да све наведене параметре (конфигурацију корисничког приступа, рачунара и мрежних уређаја) по правилу и без изузетка контролише управо клијент технолошке ревизије, што представља огроман проблем са становишта независности технолошке ревизије.

б) Екстерна технолошка ревизија

Ангажовање екстерне ревизије на први поглед у потпуности решава све проблеме у погледу независности ревизије. У погледу организационе независности и независне техничке опремљености то заиста и јесте тако, јер ревизори и клијенти припадају потпуно одвојеним организацијама.

Међутим, у организацијама у којима се буџет за ангажовање екстерне технолошке ревизије планира и контролише у секторима задуженим за управљање ИКТ, јавља се ситуација која може директно да омете независност и објективност. Наиме, јасно је да неадекватним планирањем буџета клијент ревизије може да омете или чак потпуно спречи независну и објективну ревизију у домену своје одговорности.

Проблеми који се тичу специфичних права приступа, конфигурације рачунара и мрежне опреме по правилу се отклањају током уговарања конкретног ревизорског ангажмана. Клијент се строго обавезује да испуни потребни низ техничких предуслова без којих се ревизија не може реализовати на независан и објективан начин. Тиме се ова група сметњи за независност и објективност ефективно отклања.

Постоји још један аспект независности и објективности, који је карактеристичан искључиво за екстерну технолошку ревизију. Наиме, чест је случај да се услугама технолошке ревизије баве пословни субјекти који у исто време нуде опрему, техничка решења и консултантске услуге из области технологија. По правилу, они нуде опрему само одређених произвођача, искључиво своју или оних са којима је дати субјект потписао уговор о пословној сарадњи. По истом правилу, техничка решења, технички савети и помоћ усмерени су ка опреми истих произвођача. Уколико се исти субјект налази у улогама технолошког консултанта, пројектанта, реализатора техничког решења и испоручиоца опреме (који је понекад и додатним уговором везан за редовно одржавање), онда постоји не само сметња објективности већ и очигледан сукоб интереса ако се он нађе и у улози екстерног ревизора за примењене технологије. Ово се доста често дешава, нарочито код великих понуђача, чији је обим понуде по правилу широк и разноврстан. Овај проблем може, у сопственом интересу, да реши искључиво клијент. Пре свега, подизањем сопствене свести о значају и неопходности објективне и независне ревизије информационах и комуникационих технологија а затим и доношењем информисаних одлука приликом планирања, алокације ресурса и избора одговарајућег ревизора.

2.4. РИЗИЦИ И КОНТРОЛЕ У ОБЛАСТИ ПРИМЕНЕ И КОРИШЋЕЊА ИНФОРМАЦИОНИХ И КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА

2.4.1. Пословни ризици

Најопштије речено, ризик представља могућност да дође до неког за нас неповољног исхода. Пословни ризик се огледа у могућности да неки пословни циљ не буде остварен. Пословни ентитети се непрекидно суочавају са мноштвом различитих ризика, различитих по својој природи и по свом интензитету (тј по вероватноћи реализације неповољног исхода и висини штете која би настала у случају реализације неповољног исхода).

Да би се пословни ентитет заштитио од ризика, потребно је успоставити процес управљања ризиком. Руководиоци (и ревизори) не могу никада отклонити ризик, једноставно зато што је сваки пословни подухват увек ризичан. Како се то већ каже у пословном свету – „без ризика нема добитка”. Према томе, ради се на томе да се ризици идентификују, измере, предвиде и (ако је могуће) спрече (или да се минимизују њихове последице).

Категоризација ризика нам помаже да ризике идентификујемо и квантификујемо (оценимо, тј измеримо). Такође, категоризација ризика нам помаже да успоставимо одговарајуће контроле – управљачке, оперативне и техничке мере које имају за циљ превенцију и минимизацију пословних ризика.

2.4.2. Ревизорски ризици

Ревизорски ризик је могућност да дође до грешке у ревизорским налазима, оценама и мишљењима. Грешке могу да се појаве у два смера – могући су превиди (*false negatives*), када се констатује да је у реду нешто што заправо није у реду, или „лажни аларми” (*false positives*), када се утврди да не ваља нешто што је заправо било у реду. Превиди су знатно

опаснији и представљају главнину ревизорских ризика. Ревизорски ризици су сложени и могу да се категоризују у три групе – уграђени (инхерентни) ризици, контролни ризици и ризици откривања (ризиви детекције).

Уграђени ризици (*inherent risks*) су они који су везани непосредно за саму природу посла. Наиме, као што је већ речено, сваки посао је ризичан. Међутим, неки облици пословања су ризичнији од других. На пример, вођење послова на глобалном нивоу (интернационално) је ризичније од вођења послова на локалном тржишту.

Контролни ризици (*control risks*) су они који су везани за несавршености у системима интерних контрола. Они представљају могућност да управљачко – контролни механизми једне организације неће бити у стању да на време спрече или открију неки од пословних ризика.

Ризици откривања (ризиви детекције – *detection risks*) представљају могућност да ревизија неће на време открити материјалне грешке, преварне радње итд.

Ове три врсте ризика нису међусобно независне. У процесу процене ризика, све три морају бити размотрене како би се утврдио њихов прихватљиви ниво. Не постоји могућност да се ови ризици отклоне у потпуности, али је могуће успоставити такав систем контрола који ће их држати на прихватљивом нивоу и то на трошковно ефикасан начин.

Ризик који преостане након примене контролних мера назива се резидуални ризик.

2.4.3. Информатички ризици

Ризици од присуства информатичких технологија су двојаки. Једна група се односи на могућност да се наруши тајност, доступност или интегритет информација (безбедносни ризик – *security risk*), док је друга (*IT deployment risk*) везана за могућност да се информатичке технологије уведу, примене и користе или да се њима управља на начин који је генерално неповољан по реализацију пословних циљева (ризик од умањене ефикасности, ефикасности и економичности информатичких решења).

Тајност (приватност, поверљивост) информација се односи на потребу да се приступ информацијама ограничи само на овлашћене кориснике или процесе. Свака информација се категоризује (класификује) по степену тајности, чиме се у ствари дефинише група корисника и процеса који имају право приступа тој информацији. Процеси по правилу наслеђују приступна овлашћења оног корисника који је покренуо процес (овлашћења власника процеса). Приступ се може ограничавати логички и физички. Физички приступ се односи на приступ просторијама, рачунарима и другој опреми на којој се чувају, преносе или обрађују подаци. Логички приступ се односи на приступ информатичким системима, апликацијама, базама података било локално (након оствареног физичког приступа), било удаљено (без физичког приступа, преко мрежних и других комуникационих путева). Физички приступ се ограничава физичко – техничким средствима, док се логички приступ ограничава механизмима аутентификације и ауторизације уграђеним у оперативне системе и апликације.

Интегритет информација се односи на тачност, целовитост (комплетност), ажурност и

поузданост података и информација које информациони систем производи на основу тих података. Интегритет може бити угрожен у току прикупљања, складиштења и преноса података или у току обраде информација и генерисања извештаја.

Расположивост информација се односи на потребу да информација увек мора да буде доступна овлашћеним корисницима и процесима. Појам расположивости је на изванстан начин комплементаран појму тајности – обезбеђивање приступа се мора дешавати по принципу „без овлашћења никад, али са овлашћењем увек”. Ризици од појаве проблема са расположивошћу рангирају се од једнократних и спорадичних, преко трајних али повремених (*denial of service risks*), све до фаталних, који имају катастрофалне размере (*business continuity and disaster risks*).

Ефективност, ефикасност и економичност информатичких решења може бити угрожена у било којој фази животног циклуса.

Као прво, грешке могу бити учињене у фази стратешког планирања. Стратешки план информатичког развоја мора да буде усклађен са општом стратегијом организације, тако да се уклапа у визију, мисију, циљеве и политике које је организација дефинисала. Свако одступање информатичке стратегије од генералне стратегије излаже организацију високом пословном ризику.

Кључни индикатори ризика у овој фази су: одсуство стратешког планирања, одсуство процене информатичких ризика, одсуство инвестиционе анализе, одсуство контроле квалитета, неадекватна инфраструктура, недовољна комуникација и информисање у организацији итд.

Планирање и пројектовање такође уносе специфичне информатичке ризике. Организација мора јасно да дефинише улоге и одговорности свих субјеката укључених у ову фазу. Израда плана подразумева постављање рокова, дефинисање обима пројекта (граничних услова), техничких захтева и других предуслова за квалитетно пројектовање. Пројекат генерално мора да пружи тзв предмер и предрачун – „колико нам чега треба и колико ће то да кошта”. Грешке у овој фази уносе високе пословне ризике. У принципу, грешке у стратешким одлукама, планирању и пројектовању дешавају се ређе, али остављају по правилу далеко најтеже последице. Штета је по правилу велика и тешко се надокнађује.

Кључни индикатори ризика у фази пројектовања су: изостанак одговарајуће методологије, недовољно искуство и знање руководства, тимова и појединаца, изостанак подршке највишег руководства, пропусти у прикупљању полазних информација и захтева од свих релевантних страна, недовољни ресурси (новчана средства, време, људство) итд.

У фази набавке или развоја информационих средстава и система и њихове касније имплементације потребно је такође применити стриктне мере контроле и надзора, како би се избегли карактеристични ризици.

Ако се ради о набавци, кључни индикатори ризика су: одступање од стратегије, недостатак документованих политика за набавку софтвера и хардвера, набавка без претходне анализе могућности за сопствени развој, пропусти у прикупљању

корисничких захтева, пропусти у оцени безбедности решења, одсуство анализе у домену интеграције и скалабилности решења, превиди у доменима обуке корисника, модела лиценцирања, потребне подршке и одржавања, будућих надоградњи (*upgrade*) и модификација итд.

Ако се ради о развоју, кључни индикатори ризика су: одступање од стратегије, изостанак претходне студије изводљивости, изостанак претходне анализе пословних процеса, пропусти у прикупљању захтева од руководства и/или корисника, пропусти у раздвајању развоја, тестирања и продукције система, одсуство механизма заштите и непоштовање принципа информатичке безбедности у развоју итд.

У фази имплементације система најзначајнији индикатори ризика су: изостанак разматрања алтернативних метода имплементације, непостојање документованог плана имплементације, слабости у координацији укључених тимова и појединаца, неразвијене процедуре за управљање променама, недовољна или неадекватна обука корисника, изостанак или неадекватност поступка финалног тестирања итд.

У свим фазама увођења информатичких решења неопходне су адекватне управљачко – контролне мере и стални надзор (*monitoring, supervision*) од стране руководства. Технолошка ревизија има веома важну улогу у овим процесима која се састоји у оцени адекватности ових контрола, доследности њихове примене и њихове ефективности у погледу умањења специфичних ризика.

2.4.4. Мрежни и комуникациони ризици

У условима умрежавања, који су данас практично свуда присутни, долази до појаве низа специфичних ризика, којих код засебних рачунарских система нема или су знатно слабије изражени.

Пре свега, у мрежним окружењима, поред обичних рачунара (радних станица) постоји низ различитих уређаја који су неизбежни део мрежне и телекомуникационе инфраструктуре: модеми, каблови или радио уређаји за пренос сигнала, рутери (усмеривачи саобраћаја), „свичеви” (*switch* – сабирнице и комутатори саобраћаја), приступни сервери, апликативни сервери, сервери база података, мрежни штампачи итд. Такође, софтвер је сложенији јер садржи подршку за рад у мрежи – имплементацију бројних мрежних протокола и сервиса. Према томе, мрежна окружења садрже знатно већи број потенцијалних претњи. Реални ризици су самим тим бројнији и разноврснији.

Претње којима су изложени умрежени системи могу се поделити у неколико група.

Прва група су претње физичкој инфраструктури, као што су елементарне непогоде и природне катастрофе (поплава, пожар, земљотрес и слична разорна дејства). Иако ове претње могу да угрозе и засебне, неумрежене рачунарске системе, оне су код умрежених система знатно ризичније, због просторне дистрибуције и физичке разуђености која карактерише већину рачунарских мрежа. Треба напоменути да претња физичкој инфраструктури може да наступи и од људског фактора – саботаже, диверзије итд.

Следећа група су тзв програмске (или програмиране) претње. Такву претњу представљају све врсте малициозног софтвера – вируси, црви, тројански коњи,

шпијунски и „рекламни” софтвер (*spyware, adware*), „руткитови” (*rootkits*), „ботови” (*bots, botnets*), итд.

У трећу групу спадају претње које спречавају рад система, њихових појединих делова или сервиса (*denial of service - DoS*). Иако могу постојати и на локалном нивоу (*local DoS*), ове претње су посебно изражене у мрежама, где слабости у имплементацији или конфигурацији система могу да буду искоришћене за нападе са удаљених тачака. Посебно су опасни дистрибуирани *DoS* напади, код којих се јавља тзв амплификациони (појачавачки, лавински) ефекат – мала количина мрежног саобраћаја се усмерава ка великом броју тачака у мрежи, са којих се онда синхронизовано, у исто време, покреће мноштво напада који у збиру резултирају саобраћајним преоптерећењем нападнутог система.

Друга и трећа група су директно условљене егзистенцијом тзв софтверских слабости (*software vulnerabilities*). Слабе тачке оперативних система, мрежних протокола, сервиса и апликација потичу од грешака учињених током њиховог пројектовања, кодирања или касније приликом инсталације и конфигурисања. Грешке у кодирању су врло честе и практично неизбежне, толико да већина произвођача софтвера редовно публикује исправке за своје производе (софтверске корекције, „закрпе” - енгл. *patch*). Корисници притом преузимају одговорност за примену ових корекција, често уводећи посебне контролно – управљачке процесе који служе само за те потребе (*Patch Management*). На тај начин се врши трансфер ризика са слабости софтвера на слабости у контролном процесу. Слично томе, слабости у инсталацијама и конфигурацијама контролишу посебни управљачки процеси (*Configuration and Change Management*), тако да се припадајући ризици могу третирати као да потичу од недостатака контролног процеса.

Ризици од неотклоњених софтверских недостатака често се наводе као засебна група ризика, премда су у тесној вези и међузависности са претходне две групе. Ови ризици су непосредно везани за претње од могуће злоупотребе неотклоњених софтверских недостатака. Поред злонамерног софтвера који аутоматски (програмирано) злоупотребљава „рупе” у системима, сервисима и апликацијама, злоупотребе могу бити учињене и непосредно од стране људског фактора. Нападаци различитих профила, интереса и мотивације представљају претњу која директно угрожава безбедност (тајност, интегритет, расположивост), омета функционисање система, нарушава углед организације, чини материјалну штету (увећава трошкове) и излаже организацију низу других пословних ризика.

На крају, посебна група ризика везана је за злоупотребу слабости које су својствене људском фактору. Лаковерност, неупућеност, предвидљивост људских реакција и понашања и друге особине карактеристичне за просечну личност могу бити злоупотребљене од стране нападача. Преваре, манипулације, дезинформације, лажно представљање и слично, у условима умреженог пословања, где је чест случај пословних контаката са особама са којима се никада нисмо физички сусрели и упознали, добијају врло повољне могућности за успех. У новије време, о овој врсти ризика се доста пише, најчешће под називом „социјални инжињеринг” (*social engineering*). Међутим, у ову групу могу да се сврстају и неке претње које уско гледано не спадају у социјални инжињеринг, али се такође базирају на злоупотреби људске слабости, као што су ширење дезинформација (*hoax*), подметање лажних адреса, сервера и сервиса (*phishing*) и слично.

На крају, треба рећи да је овде изложена категоризација ризика у великој мери поједностављена и да никако не може бити узета као коначна или једина могућа. Ипак, она може да послужи не само као илустрација основног појма ризика, већ чак и да олакша идентификацију главних ризика услед присуства ИКТ у неком реалном пословном окружењу.

2.4.5. Контроле и системи интерних контрола у ИКТ

Потреба за контролом у пословним процесима стара је колико и само пословање. Међутим, теоријске основе и прва систематизована практична упутства постављају се тек у новије време. У свом извештају из 1992. године, организација COSO поставља теоријску основу за системе интерних контрола. Иако изворно амерички, овај материјал убрзо постаје интернационално прихваћен. Следе слични подухвати у низу других земаља: В.Британији (*Cadbury Report*), Канади (*CoCo*), Француској (*Vienot Report*), Јужној Африци (*King Report*) итд.

У свим овим извештајима дају се најопштије дефиниције интерне контроле као процеса који има за циљ одржавање и унапређење ефикасности и ефикасности пословних операција, поузданости финансијског извештавања и усклађености са законима и другом регулативом. Веома значајно је и то што се интерне контроле у свим овим документима јасно постављају у оквиру непосредне одговорности руководства. Контрола је препозната као саставни део процеса управљања и не може бити делегирана другим ентитетима, па тако ни интерној ревизији.

Поред ових најопштијих оквира, развијају се и оквири за поједине уже области контроле, као што су контрола ризика, контрола квалитета итд.

У области примене и коришћења информационих и комуникационих технологија најдетаљнију разраду пословних процеса и припадајућих контролно – управљачких механизма даје организација ISACA у својим смерницама под називом COBIT. Прва верзија је настала 1996. године. Велики успех и глоблну прихваћеност COBIT доживљава након 2000. године, када је публикована верзија 3.0. Данас је актуелна верзија 4.1, у којој је препознато 4 домена, у њима 34 процеса са укупно 318 активности, са исто толико дефинисаних контролних смерница. Нешто више о оквирима COBIT и COSO дато је у делу 2.20 – „Професионална регулатива, стандарди, препоруке и радни оквири”.

2.4.6. Класификација интерних ИКТ контрола

Интерне контроле у области примене и коришћења технологија могу да се класификују на више начина.

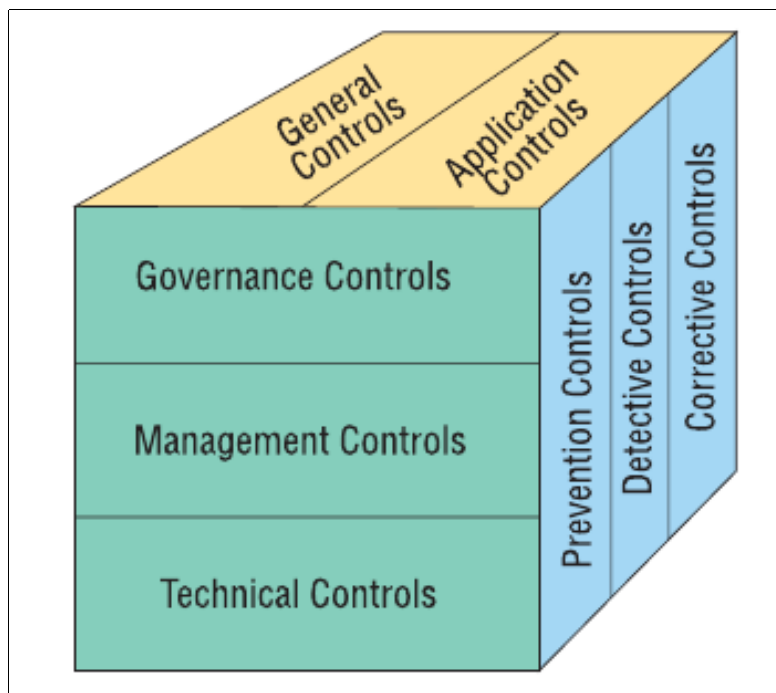
Једна веома упрошћена подела већ је коришћена раније у овом раду. То је подела на опште (генералне) и апликативне контроле. Та подела илуструје основну двојност интерних контрола у области ИКТ. Наиме, једним делом ИКТ контроле служе као подршка управљању и управљању пословним процесима који су имплементирани у информационим системима и пословним апликацијама, док другим делом ове контроле служе за управљање самом технолошком инфраструктуром, као подршка делу организације који је одговоран за примену и коришћење информационих и

комуникационих технологија.

Остали примери могуће класификације интерних контрола су поделе на ручне и аутоматске (*manual, automatic*), обавезне и опционе (*mandatory, voluntary*), комплементарне (редундантне) и компензационе (*complementary, redundant, compensating*), непрекидне, „на захтев” и „по догађају” (*continuous, on-demand, event-driven*) итд.

Постоје врло детаљне и свеобухватне класификације, попут оне коју даје *COBIT*, које су намењене практичној примени у великим и сложеним организацијама. Такве примене захтевају широк обим претходних знања и искустава, што често подразумева и специјалистичку обуку.

Међутим, за оквире овог рада биће нам довољна знатно једноставнија класификација, али довољно елаборирана да омогући добар увид и правилно разумевање интерних контрола у контексту ИКТ. Једна таква класификација дата је у публикацији Института интерних ревизора (*IIA*) под називом *Information Technology Controls (GTAG-01)* [32]. Та класификација даје троструку поделу, па се као илустрација користи графички приказ у три димензије (коцка). Слика 1 је преузета из GTAG-01. На њој је приказана трострука подела: у једној равни је подела на генералне и апликативне контроле, у другој на превентивне, детективне и корективне, док је у трећој подела према нивоу овлашћења и одговорности за успостављање и примену контрола: највише управљачке контроле, контроле у нивоу руководства и техничке контроле.



Слика 1: Интерне контроле у ИКТ системима

а.1) Опште (генералне) контроле

Ове контроле су познате и под називом инфраструктурне контроле. Оне се односе на све системске компоненте и процесе у примени и коришћењу ИКТ и припадајуће податке

релевантне за дату организацију или окружење. Оне, између осталог, укључују политике информатичке безбедности, администрацију система, приступ систему и његовим компонентама, раздвајање (сепарацију, сегрегацију) дужности код кључних ИКТ функција, управљање набавком, развојем, имплементацијом и конфигурацијом, управљање променама у систему, управљање применом системских корекција (*Patch Management*), контроле за непрекидност пословања и опоравак од инцидената, израда резервних преписа (резервне копије – *backup*), процедуре за њихову примену код системског опоравка (*recovery*) итд.

а.2) Апликативне контроле

Као што је већ помињано, апликативне контроле се односе на механизме уграђене у информационе системе и апликативну логику, а који служе као подршка управљању и контроли пословних процеса. Ту спадају, између осталог, контроле за валидацију поља за унос података, контроле ауторизације за приступ сегментима пословних апликација, раздвајање (сегрегација) пословних функција, контроле тачности разних обрачуна, регистровање трагова о трансакцијама, извештаји о грешкама итд.

б.1) Превентивне контроле

Превентивне контроле имају за циљ да спрече настајање догађаја неповољних по организацију и њене циљеве. Пример превентивних контрола су контроле за валидацију уноса података. У поља за унос нумеричких података не сме се дозволити унос знакова који нису цифре – слова, интерпункција, контролни знакови и сл. Други пример су контроле за ауторизацију приступа које спречавају приступ неауторизованим корисницима итд. У превентивне контроле такође спадају и комплексни кориснички софтвер, уређаји и системи, као што су анти-вирусни софтвер, мрежне баријере (мрежне запреке, заклони – *firewalls*), системи за превенцију упада (*Intrusion Prevention Systems – IPS*).

б.2) Детективне контроле

Детективне контроле откривају неповољне догађаје (грешке, инциденте и сл.) након што су се они већ десили. Циљ ових контрола је да открије настале проблеме и укаже на њих пре него што дође до ескалације њихових штетних последица. На пример, детективне контроле могу да идентификују неактивне рачуне или рачуне са сумњивим активностима. Такође, детективне контроле могу да буду задужене за праћење разних индикатора преварних радњи, пробијања лимита код трансакција, нетачности у обрачунима итд. Поред апликативних, детективне контроле могу да буду и у групи општих контрола – детекција грешака у комуникацији, детекција нарушеног интегритета система фајлова, детекција упада у систем (*Intrusion Detection Systems – IDS*), детекција употребе неаутентификованих, истеклих или повучених дигиталних сертификата, итд.

б.3) Корективне контроле

Корективне контроле служе да се отклоне слабости, грешке и пропусти које су довеле до неповољних догађаја. Оне се крећу од врло једноставних, као што су просто отклањање грешака на уносу података, преко укидања налога за приступ корисницима који су покушали или реализовали неауторизовани приступ, опоравка грешком избрисаних података применом резервне копије, па све до најсложенијих, као што је активирање резервних система за непрекидност пословања у случају озбиљнијих инцидената, отказа појединих компоненти или потпуног уништења система.

в.1) Контроле на нивоу највише управе (*Governance*)

Ова група обухвата контроле за чије успостављање, примену и функционисање одговара највиши ниво управе у организацији: управни одбор, генерални директор, руководиоци највишег нивоа и други органи управе са највишим нивоом овлашћења и одговорности.

У домену примене и коришћења технологија, контроле овог нивоа обухватају, поред осталог, и следеће: стратешке смернице, политике за примену и коришћење технологија, политике за информатичку безбедност, мере којима се обезбеђује надзор над одвијањем пословних процеса, мерење и оцене ризика, мерење и оцене успешности пословања итд.

У најопштијем смислу, читава пословна функција интерне ревизије представља такође једну из ове групе контрола.

в.2) Контроле на нивоу руководства (*Management*)

Овде спадају контроле за чије успостављање, примену и функционисање одговарају извршни руководиоци у организацији. На први поглед је тешко повући границу између ове и претходне групе. Међутим постоји једноставно правило за дистинкцију: за руководиоце из претходне групе у погледу интерних контрола важи правило „*Noses in – fingers out*”, што је жаргонски израз за принцип по коме је руководство из групе в.1 задужено за надгледање, праћење и давање општег усмерења али не и за реализацију. За разлику од извршног руководства, које има овлашћења и одговорности и за доношење и за спровођење конкретних пословних одлука, највиша управа у спровођењу уопште не учествује.

У домен ових контрола спадају управљање ризиком, контрола усклађености са законима, осталом интерном, екстерном регулативом и уговорима, спровођење политика, процедура, контроле радног окружења и безбедности на раду, управљање пројектима, итд.

в.3) Техничке контроле

Техничке контроле представљају најнижи и у исто време основни ниво контрола у области примене и коришћења технологија. Оне су темељ сваког система интерних ИКТ контрола и обезбеђују основу за поузданост функционисања практично свих осталих контрола у једној организацији.

На овом нивоу се заправо остварује непосредна (физичка и/или логичка) реализација свих контрола које су креиране и прописане на вишим нивоима. Треба напоменути да су ове контроле зависне од индивидуалних технологија и техничких решења која су на њима заснована, што са контролама вишег нивоа најчешће није случај.

Уколико организација обезбеди ефективан и ефикасан систем контрола на техничком нивоу, испуњен је један од најкритичнијих фактора успеха за укупан систем интерних контрола. Такође, по самој својој природи, техничке контроле се могу у великој мери аутоматизовати. Искључењем ручних контрола са техничког нивоа и оптимизовањем аутоматских контрола, организација може да постигне веома висок степен заштите од ризика.

Поред тога, препознавањем значаја контрола техничког нивоа и њиховим укључењем у предмет ревизије, технолошка ревизија може да додатно и врло значајно увећа свој

допринос укупним вредностима организације.

2.5. ПРОЦЕС РЕВИЗИЈЕ И РЕВИЗОРСКЕ АКТИВНОСТИ

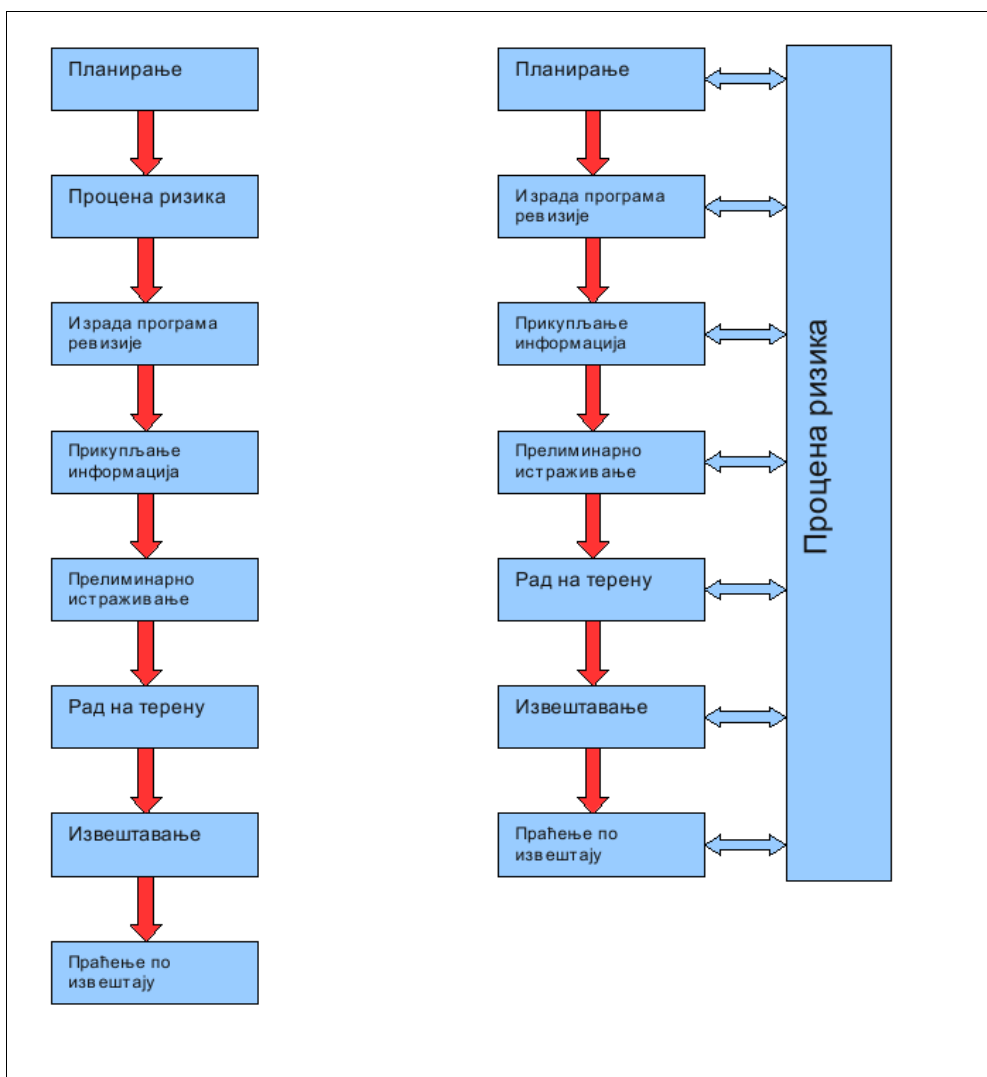
2.5.1. *Животни циклус процеса ревизије*

Процес ревизије је непрекидан и има кружни ток. Он има неколико препознатљивих фаза које се смењују у току животног циклуса. Процес почиње планирањем, наставља се неком врстом припреме, непосредним извођењем ревизорског задатка (радом на терену), изработом и предајом извештаја и завршава се даљим праћењем по извештају. Овај циклус се затим континуирано понавља. Треба рећи да у литератури постоје разлике код дефинисања појединих фаза. Најчешће, разлике су у резолуцији детаља којом се циклус приказује: поједине фазе се приказују као секвенца од две или више детаљнијих фаза или обратно, што се своди на различит број фаза у циклусу. Поред тога, често срећемо и различите називе појединих фаза.

Међутим, можда је једина суштинска разлика у томе што се код различитих аутора срећу различита схватања у погледу места коју у циклусу треба да има процена ризика.

2.5.2. *Процена ризика*

У савременим организацијама често срећемо засебне организационе целине које се баве тзв управљањем ризиком (*Risk Management*). управљање ризиком је крајем прошлог века па до данас прошло кроз убрзан и снажан развојни процес и достигло статус веома значајне компоненте сваког пословања, па чак и засебне стручне гране са самосталном стручном теоријом и праксом. Развијени су многи радни оквири и методологије за категоризацију, идентификовање, процену и мерење, као и за минимизацију, избегавање, трансфер и друге начине за контролу и управљање ризиком. Спремност за реаговање у ситуацијама када дође или може доћи до исхода негативних по пословне циљеве уграђује се данас у стратешке и оперативне планове свих успешних организација.



Слика 2: Животни циклус технолошке ревизије

Иако управљање ризиком није у области директне одговорности интерне ревизије, ревизорски посао је нераскидиво везан за процену ризика.

Уобичајено је да се процена ризика сматра посебном фазом у животном циклусу ревизије, која долази непосредно пре или непосредно после фазе планирања. У новије време често се користи фраза *Risk-based* (или *Risk-driven*) *Auditing*, чиме се жели истаћи да је одређени ревизорски приступ заснован на ризику или је вођен ризиком.

Доследно гледано, ако заиста желимо да се ревизорски посао одвија са пуном свешћу о присутним ризицима, онда је вероватно најисправнији приступ код којег све фазе животног циклуса ревизије укључују и процену ризика као свој саставни део. Заиста, до сазнања о слабостима и недостацима предметног система услед којих смо изложени ризицима, може се доћи у свакој фази ревизије. У свакој од фаза ревизије процена ових ризика може и треба да утиче на евентуалне модификације у даљем току одвијања ревизорског циклуса. Слика 2 илуструје ток животног циклуса ревизије и место процене ризика у њему.

2.5.3. Планирање

Планирање ревизије представља први корак у сваком конкретном ревизорском задатку.

Дугорочно планирање се по правилу одражава кроз израду годишњег плана рада, у којем се дефинишу циљеви, предмет, ресурси, опсег и трајање за одређени број конкретних задатака на којима ће ревизори бити ангажовани у предстојећем једногодишњем периоду. Овај план предлаже руководилац интерне ревизије а усваја га одбор за ревизију, генерални директор или други орган највише управе којем је интерна ревизија одговорна. Годишњи план мора да буде у складу са стратегијом, пословним циљевима и потребама организације. Такође, садржај годишњег плана рада се мора ускладити са претходно процењеним ризицима у организацији. Пошто су ресурси по правилу ограничени, ревизија није у могућности да „ради све”, већ мора да се фокусира само на најважније области, тј на оне које су приоритетне са аспекта *вероватноће наступљања и штељивости последица* неповољних исхода.

Краткорочно планирање се одражава кроз израду краткорочних планова и кроз планирање појединачних ревизорских пројеката. Док је израда краткорочних планова необавезна и не тако честа, планирање индивидуалних пројеката је обавезна активност за сваку интерну ревизију. Током ове активности ревизори доводе у везу индивидуалне ставке из годишњег плана са конкретним условима у датом окружењу и у датом моменту (периоду времена). Ревизорски пројекат се синхронизује са текућим активностима клијента ревизије, поново се разматрају циљеви, ресурси опсег и трајање ревизије, како би се ускладили са реалношћу текућих пословних процеса.

Овде треба напоменути да је дугорочно и краткорочно планирање карактеристично (и обавезно) за тзв системски приступ ревизији. За разлику од системског, постоје и други приступи, који могу бити примењени у зависности од природе конкретног ревизорског задатка. На пример, поред редовних ревизија, где се задаци планирају унапред, постоји и могућност ангажовања ревизора на тзв ванредним ревизијама. Код оваквих задатака врло често није могућ системски приступ, већ се послу приступа као да је реч о појединачној, ад-хок истрази.

Примери су врло бројни – ту спадају све ревизије откривених или наговештених преварних радњи, све ревизије по инцидентним ситуацијама, ревизије по дојавама (*whistleblowing*), жалбама корисника итд. У области технолошке ревизије, због специфичности предмета ревизије, истражни приступ се веома често користи. За све такве случајеве, по правилу, постављају се високи приоритети реализације и веома кратки рокови. Процес планирања се тада нужно своди на краткотрајне тактичке припреме, после чега се прелази на следећу фазу – израду програма ревизије (види 2.5.4). Није редак случај да код оваквих задатака дође до значајног одступања од годишњег плана, прерасподеле ресурса, прекида текућих или одустајања од планираних (редовних) ревизорских задатака и других сличних последица. Оне у општем случају доводе до увећања ревизорских ризика, али се полази од оцене руководства (разумног очекивања) да ће то, кроз резултате ревизије, да буде компензовано минимизирањем неког другог пословног ризика, у укупном износу који је позитиван за организацију.

2.5.4. Израда програма ревизије

За сваку појединачну ревизију (конкретан ревизорски задатак) неопходно је претходно израдити детаљан програм. Овај програм се израђује како за редовне (планиране) тако и за ванредне ревизије. Сврха програма ревизије је да обезбеди сређен и систематичан приступ предмету ревизије, тако да се избегне могућност да дође до пропуста, грешака у поступку, одступања од задатих циљева или других ревизорских ризика. Програм ревизије успоставља везу између општих ревизорских активности усаглашених са опсегом и циљевима конкретне ревизије са једне стране и расположивих стручних и других ресурса са друге стране.

Програм ревизије најчешће има два дела. У једном, који служи као заглавље целог програма, идентификују се и наводе клијенти ревизије, предмет ревизије, опсег рада, циљеви, име одговорног ревизора и чланова ревизорског тима, времена и рокови. У другом делу се садржи конкретна секвенца ревизорских активности. Она повезује ревизорске активности планиране за сваку од фаза ревизије са клијентима ревизије, планираним временским оквирима, ревизорима који обављају ту активност, евентуалним додатно захтеваним ресурсима и (по потреби) са другим општим напоменама.

Програм ревизије до детаља прати ток одвијања конкретног ревизорског задатка и служи ревизору као контролно средство – подсетник за обављање ревизије – којим се додатно обезбеђује да ревизија успешно испуни планиране циљеве. Програм ревизије уважава резултате претходне процене ризика, тако што планира активности по приоритетима у складу са том проценом.

2.5.5. Упознавање са предметом ревизије

Циљ упознавања са предметом ревизије јесте да се изврши адекватна припрема и прикупе све полазне информације које су неопходне за успешно извођење ревизорског задатка. Такође, у овој фази, ревизор је дужан да идентификује предметни систем и њему припадајуће организационе целине, као и носиоце руководећих улога и одговорности у тим целинама.

Конкретно, ревизор је дужан да прибави и прегледа следеће:

- све постојеће претходне оцене, а које се односе на предметни систем. Ово обухвата претходне извештаје интерне и/или екстерне ревизије, претходне процене припадајућих ризика, евентуалне техничке и административне контроле, извештаје инспекција и све друге извештаје о стању предметног система који су релевантни за дати ревизорски задатак
- све законе, прописе и подзаконска акта који се односе на предметни систем и применљиви су на датом ревизорском задатку
- интерну регулативу – политике, правилнике, процедуре и друго што је применљиво на датом ревизорском задатку; уколико је то применљиво на конкретном задатку, потребно је прибавити и све уговоре који се односе на предметни систем
- професионалну регулативу – смернице, стандарде, радне оквири за најбољу професионалну праксу и друго што је применљиво на датом ревизорском задатку

- друга релевантна документа и информације, применљиве на предметни систем, као што су дефиниције граничних линија предметног система, узајамне везе са другим системима и сл

Након прегледа прикупљених информација, ревизор припрема најаву ревизије. Најава мора да садржи:

- Предлог предмета ревизије – циљеве и опсег ревизије
- Време почетка и процену трајања ревизије
- Име надлежног ревизора и податке за контакт

Директор интерне ревизије одобрава најаву и шаље је клијентима.

Следећа активност је заказивање и одржавање уводног састанка са сваким од клијената, како би се дискутовало и постигао договор о коначном подручју и циљевима ревизије, евентуалним променама у том погледу, кључним контактима, времену ревизије и особљу које ће је обавити. Ревизор је у обавези да сачини белешке са ових састанака.

2.5.6. Прелиминарно истраживање

Циљ прелиминарног истраживања јесте да се постигне разумевање предметног система, његових пословних и контролних процеса, циљева, пратеће регулативе и подручја одговорности. Током ове фазе, ревизор стиче основна сазнања о предмету ревизије, тако што проучи сва релевантна документа која је прикупио, спроведе потребне разговоре и посматра и анализира процесе рада и функционисање предметног система. У току ове анализе, ревизор идентификује основне процесе предметног система, јаке и слабе тачке сваког од тих процеса и означава их за каснију детаљну проверу и тестирање према процењеном степену ризика који им припада.

У овој фази, програм ревизије се допуњава детаљима реализације рада на терену, који садржи појединости о проверама и тестовима које треба обавити. Ту се специфицирају методе, технике и алати, процењено трајање и очекивани резултати – конкретни циљеви које рад на терену треба да испуни.

2.5.7. Рад на терену

Циљ ове фазе је да се прикупи, анализира, протумачи и документује свака релевантна информација како би се коначни резултати ревизије подржали аргументима и испунили постављени циљеви ревизије.

Најважнија активност у овој фази јесте обављање свих потребних провера и тестирања. Резултате ових провера и тестова потребно је продискутовати са клијентом ревизије, како би се избегла евентуална необавештеност клијента и обезбедила потврда исправости резултата.

Оперативно гледано, ово је централна активност сваке технолошке ревизије. Током ње се формира коначна листа главних ревизорских налаза. На основу резултата ове фазе формирају се закључци, мишљења, оцене и препоруке корективних мера, дакле сви најважнији резултати ревизије.

Назив „рад на терену” води порекло из традиционалне ревизије. У контексту технолошке ревизије не треба га схватити дословно. У условима умрежености, већина активности из фазе „рада на терену” може се обавити „на даљину”, уз употребу погодних техника и алата. Мапирање мрежа, енумерација уређаја, енумерација и идентификовање сервиса, оперативних система и апликација, откривање слабости и други поступци у овој фази могу бити обављени на аутоматизован начин и у већини случајева са једне централне локације у мрежи.

Резултат ове фазе јесте резиме налаза и закључака. Они се рангирају према степену припадајућег ризика и чине основу за израду ревизорског извештаја. Пре него што се приступи изради извештаја, резиме рада на терену је пожељно продискутовати са клијентима ревизије, ради коначног усклађивања.

2.5.8. Извештавање

Циљ ове фазе је да се саопште крајњи резултати ревизије – налази, закључци, мишљења и препоруке.

Извештавање у општем случају има два корака – израда и одобрење нацрта извештаја и израда коначног извештаја. Нацрт извештаја се даје на преглед и одобрење руководиоцу интерне ревизије. Корекције које након прегледа наложи руководилац улазе у коначан извештај.

Ревизорски извештај има дводелну структуру. Први део је резиме (*executive summary*) у којем се укратко излажу најважнији резултати ревизије: закључци, мишљења, оцене и препоруке корективних мера. Резиме такође може да садржи и најважније ревизорске налазе ако је то потребно, ради аргументације у прилог изнесених резултата. Обим резимеа је по правилу не већи од две до три стране текста. Други део је детаљни ревизорски извештај у којем се детаљно излажу налази ревизије везани за слабости које је потребно кориговати. У контексту технолошке ревизије, детаљни извештаји могу имати обим од више десетина, па чак и више стотина страна текста.

Једноставно правило по којем се разграничава садржај ова два дела извештаја је следеће: у резиме се стављају информације које су од интереса за највише руководство и генералног директора, док се у детаљни део извештаја стављају информације од интереса за ниже руководство и извршиоце непосредних корективних мера.

Директор интерне ревизије коначни извештај шаље наручиоцу ревизије (одбор за ревизију, генерални директор и сл.) и клијентима ревизије – руководиоцима свих организационих целина које су биле захваћене ревизијом.

2.5.9. Праћење по извештају

Завршна (и у пракси најчешће занемаривана) фаза јесте фаза праћења по извештају. Циљ ове фазе јесте да се обезбеди уверење да ће препоручене корективне мере из ревизорског извештаја заиста и бити спроведене.

Након пријема извештаја, клијент је у обавези да сачини план имплементације

корективних мера и да га достави ревизору. На основу овог плана, који мора да буде усклађен са расположивим ресурсима клијента и са проценом ризика, ревизор планира рокове у којима ће обавити контролу реализације за сваку од препоручених мера.

2.5.10. Конвенционални и стриктно технолошки приступ – главне разлике и могућности интеграције

У уводном делу (2.1. Увод) већ је помињана двојност приступа технолошкој ревизији која се огледа у постојању две међусобно независне „школе”: једна, пореклом из традиционалне ревизије, финансијски оријентисана ревизија и друга, пореклом из информатике, технички и технолошки оријентисана ревизија. Разлике између ових приступа су највидљивије у третману интерних контрола и појединих ревизорских активности током животног циклуса интерне ревизије. Стога контекст интерних контрола и одговарајућих ревизорских поступака представља и најпогодније место за детаљније разматрање најбитнијих разлика.

Разматрању најзначајнијих разлика приступићемо са идејом да се истакну могућности за њихово комбиновање и међусобно допуњавање и за изградњу једног модерног, интегрисаног приступа технолошкој ревизији.

а) Разлике у третману процене ризика

Конвенционална ревизија покушава процену ризика да прикаже као једну од фаза у животном циклусу ревизије. Често се процена ризика приказује као фаза која претходи фази планирања. Мотивација за то је јасна и логична – заиста је пожељно познавати ризике пре него што се донесу било какве одлуке о предмету ревизије – циљевима и опсегу ревизорских пројеката и задатака. Пошто се циљеви и опсег дефинишу управо у фази планирања, јасно је да би пре тога било упутно обавити неку врсту процене ризика.

Међутим, исто тако је јасно и логично да се и циљеви и опсег, као и други параметри утврђени планом могу (често и морају) мењати током каснијих фаза у животном циклусу ревизије. Са сваком следећом фазом расте опсег и квалитет ревизорских сазнања о предмету ревизије. Нова запажања, закључци и оцене могу у значајној мери да одступају од иницијалних процена и претпоставки.

Тако се долази до идеје да се нека врста процене ризика мора вршити током целог циклуса. Свака од фаза мора да дозволи промене у постављеним приоритетима, без обзира на иницијални садржај плана. Овај концепт је одавно познат технолошким ревизорима који раде у информатичким окружењима. На пример, при скенирању сервисних портова на серверима и радним станицама (што се, према конвенционалној ревизији, догађа тек у фази рада на терену) може се утврдити да је на једној од радних станица које припадају развоју присутна нека слабост која може бити искоришћена за напад на продукциони систем. Према томе, процена ризика у фази рада на терену може нам дати сасвим другачије резултате од оне процене ризика која је претходила планирању. Сличним примерима може се показати да исто важи и за све остале фазе у циклусу.

Интегрисани приступ процени ризика у технолошкој ревизији илуструје дијаграм десно на Слици 2.

б) Системски приступ и приступ путем једнократне пробе (истраге)

Конвенционална ревизија фаворизује системски приступ. Сви ревизорски пројекти и задаци се најпре планирају, па се према усвојеном и одобреном плану приступа њиховој реализацији – према добро уходаној шеми животног циклуса.

Међутим неки ревизорски задаци су по својој природи неподесни за системски приступ. Инцидентне, неочекиване ситуације налажу ванредан ревизорски третман, који више личи на истрагу него на редовну ревизију. По правилу, такви задаци су хитни, морају бити обављени одмах, резултати се очекују у најкраћем року, тако да не могу бити темељно и систематски планирани. Шта више, они често изискују промптне измене постојећег плана, одлагање или чак отказивање других редовних и планираних ревизија.

У информатичким окружењима овакве ситуације су релативно честе, добро познате па чак и очекиване, покривене одговарајућим контролама. Ревизори који раде у таквим окружењима често добијају задатке да изврше неки појединачни тест или проверу. Примери су бројни: ревизија информатичке безбедности одређеног веб сајта, ревизија изворног кода неке апликације, тест на пробој (*penetration test*) неког продукционог система, итд. Честе су и пост-мортем ревизорске анализе, као на пример након испада неког система или неке његове компоненте, анализе штете после инцидента, утврђивање узрока инцидента, одговорности за инцидент итд. Овакви задаци често укључују потребу за посебним знањима, техникама и алатима (етичко хаковање, дигитална форензика и сл.).

Учестаност ситуација које изискују овакав приступ и његова незаменљивост у таквим ситуацијама намећу потребу да се ревизорски профил прошири изван конвенционално – системског и интегрише са ванредно – инцидентним приступом.

в) Неформална и континуална ревизија

Потреба за одступањем од строго планског и систематског приступа није условљена само ванредним и инцидентним ситуацијама. Модерно пословање се одвија у условима сталних промена. Брз технолошки развој, конкурентска борба, нове услуге и производи, императив за оптимално коришћење ресурса и низ сличних фактора уносе висок степен динамике и условљавају брзо реаговање и прилагођавање променама у свим пословним процесима. Код руководиоца расте тзв „апетит за ризик” (*risk appetite*) – износи преосталог ризика у модерним и динамичним организацијама у данашње време подижу се до нивоа који су донедавно сматрани неприхватљивим. Од тога није поштеђена ни интерна ревизија.

Постоје два начина да се одговори на овакву врсту изазова. Први је увођење елемената неформалне ревизије а други је тзв континуална ревизија. Оба начина су примерена технолошкој ревизији и врло применљива у неким од њених задатака.

Ограничења ресурса су довела до развоја ревизије која се руководи ризиком. Као што је већ речено у 2.5.2 и 2.5.3 ревизија која „не може да ради све” усмерава се тако да ради оно што је најкритичније у погледу ризика којима се организација излаже. Међутим, ту постоји следећи проблем: ако се ревизија у своме раду искључиво руководи ризиком,

онда је очигледно да она неке области пословања никада неће прегледати и анализирати. Једноставно, на њих никада неће доћи ред, пошто се никада не налазе на листи најризичнијих области.

Показује се да неформална и континуална ревизија могу да буду од велике користи и у решавању овог проблема.

Неформална ревизија је приступ у којем се свесно одустаје од неких елемената дисциплине, систематичности и детаљности који су иначе својствени конвенционалној ревизији. Ако је ревизор стручно оспособљен и има потребна знања, вештине и искуство, руководиоца може да му дозволи да поједине задатаке обави без претходне процене ризика, без детаљног и документованог плана и без обавезе да строго и систематично документује све налазе, формира радне папире и слично. Статистичко формирање узорака се такође прескаче и уместо тога узорци се формирају емпиријски, према претходним сазнањима и личном уверењу ревизора. Радни налог га обавезује да сачини кратак и концизан извештај у задатом року, што представља апсолутни минимум формализма.

Ако се примени правилно и на местима где је одговарајући, овакав приступ може да пружи врло квалитетне резултате. Јасно, од неформалне ревизије не могу се очекивати целовити и свеобухватни извештаји, али пракса показује да је управо тај приступ успевао да открије многе слабе тачке које су претходно промакле темељно вођеним анализама ризика.

Континуална ревизија је приступ у којем се неке провере и тестови обављају непрекидно, по правилу аутоматски, и то у циклусима који су независни од редовног циклуса ревизије. Овакав начин провера и тестова веома је применљив у разним областима технолошке ревизије, под условом да ревизори поседују потребне компетенције и да су опремљени потребним алатима. Најчешће, овакав приступ се заснива на примени неких софтверских сензора, агената или аутоматских скенера, али постоје и друга решења (хардверски уређаји – *audit appliances*). Њиховом применом, технолошка ревизија поприма нека својства сталног праћења (мониторинга). Поред техничких компетенција, за континуалну ревизију је неопходно и врло детаљно разумевање контролног окружења и свих правила и изузетака у системима интерних контрола.

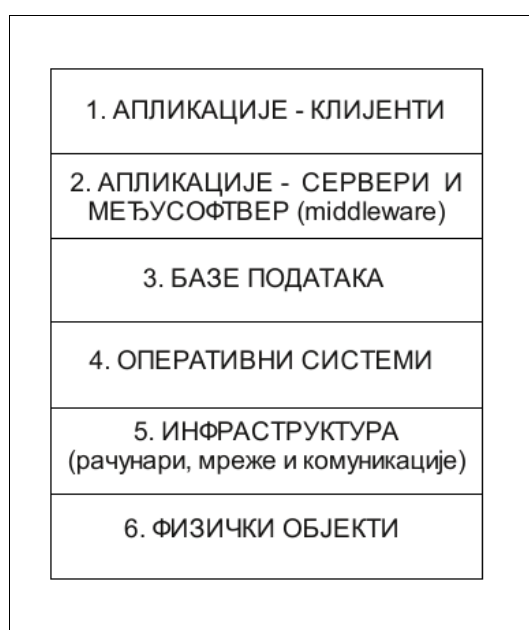
Континуалну ревизију илустроваћемо једним примером: у организацији која има имплементиран систем за управљање софтверским корекцијама (*patch management*), технолошки ревизори често користе софтверски скенер који непрекидно тестира све рачунаре у систему у погледу примењених софтверских „закрпа” и сервисних пакета апликативног и системског софтвера. Кратки извештаји из овог програма могу се добити на крају сваког циклуса тестирања, периодично, или у реалном времену, у форми аларма.

г) Провере и тестови

Вероватно најбитније разлике између конвенционалног и стриктно технолошког приступа уочавају се код практичних провера и тестова који се одвијају у фази рада на терену.

У свом раду на терену, конвенционална ревизија фаворизује посматрање процеса и функционисања система, разговоре са одговорним лицима, упитнике, интервјуе и сличне методе за проверу. Егзактна тестирања се најчешће врше на статистички изабраним узорцима, чијом анализом се долази до налаза и показатеља на основу којих се онда извлаче закључци.

Апликативне и опште контроле се редовно проверавају и тестирају, али углавном на нивоу контрола за које одговарају руководиоци – средњег или највишег нивоа. У домену техничких контрола (види „коцку” у одељку 2.4.6. *Класификација интерних ИКТ контрола*), конвенционална ревизија скоро да не ради ништа. Колико је озбиљна и значајна ова „слепа тачка” види се са Сlike 3, на којој је детаљно приказана дубина и сложеност подручја у којем се техничке контроле простиру.



Слика 3: Подручја обухваћена техничким контролама

Област техничких контрола које успева да обухвати конвенционална ревизија према овој слици једва да излази из апликативног нивоа (слојеви 1 и 2). У области генералних контрола, које су најчешће заједничке за цео ентитет и које су по правилу централизоване, то може бити и нешто шире, али и тада се не иде у потребну дубину. Већ је речено да ниво техничких контрола има фундаментални значај за целокупни систем интерних ИКТ контрола. Док виши нивои контрола дају усмерење, прописују мере и брину о томе да ли у систему интерних контрола „постоји све што је потребно”, дотле техничке контроле брину о томе да ли заиста и „све функционише како треба”. Према томе, одсуство увида интерне ревизије у детаље техничке и технолошке природе представља велики недостатак и извор је изузетно високог инхерентног ревизорског ризика.

Ово вероватно представља највећи проблем који конвенционална ревизија има у области

примене и коришћења информационих и комуникационих технологија.

Срећом, то је уједно и област у којој постоји највећа прилика за развој интегрисаног приступа. Наиме, за технолошке ревизоре који долазе из информатичког окружења управо ова област представља центар професионалног интересовања и домен у којем доминантно долазе до изражаја њихова стручна знања, вештине и искуства.

Уколико организација успе да integriше конвенционалну и информатичку ревизију у нивоу ревизије техничких контрола и притом постигне усклађеност и равнотежу оба ревизорска профила у својим ревизорским тимовима, тиме ће бити испуњен најважнији од свих кључних фактора успеха за њене процесе технолошке ревизије и истовремено отклоњен један од најзначајнијих извора инхерентног ревизорског ризика.

2.6. ПОСЕБНЕ ОБЛАСТИ ТЕХНОЛОШКЕ РЕВИЗИЈЕ

2.6.1. Ревизија информатичке безбедности

Ревизија информатичке безбедности је технолошка ревизија која се бави безбедношћу информационих и комуникационих технологија и система који су на њима засновани. У ери опште информатизације свих видова пословања питања информатичке безбедности су по правилу везана за врло високе пословне ризике. Са друге стране, савремена технолошка ревизија је управо базирана на ризику и тежи томе да се у што већој мери руководи проценом ризика. Због тога је ревизија информатичке безбедности стално присутна и представља нераскидиви, ако не и најважнији део сваке технолошке ревизије. Практично сваки задатак технолошког ревизора има присутне и бар неке елементе ревизије информатичке безбедности.

Међутим, упркос томе што се стално преплиће са општом технолошком ревизијом, због специфичних знања, вештина, техника и алата који се користе у овој области, она се често разматра и третира потпуно одвојено од остатка технолошке ревизије. Велики број организација се одлучује да услуге ревизије безбедности тражи са стране, од независних, екстерних специјалиста, којих у свету има све више.

Слично општој технолошкој ревизији, ревизија информатичке безбедности такође се бави контролама и то у више нивоа: административним (управа и руководство), техничким и физичким. Постоји много ужих дисциплина издиференцираних унутар ревизије информатичке безбедности, посебно у нивоу техничких контрола. Тако постоје засебне ревизије безбедности веб апликација, база података, мрежа, мрежног перимтра и демилитаризоване зоне, оперативних система итд.

2.6.2. Ревизија преварних радњи и место дигиталне форензике у технолошкој ревизији

Иако многе организације имају потребу да успоставе засебне организационе целине специјализоване за борбу против разних преварних радњи (*Fraud Management*), код већине организација то ипак није случај. Када величина, сложеност или природа посла организације не оправдава увођење посебних служби за то, онда је спречавање, откривање и реаговање на откривене преваре препуштено општим системима интерних контрола у организацији.

Улога ревизије у овим процесима је онда врло слична улози коју ревизија иначе има у оцени система интерних контрола. Међутим, у неким аспектима, ревизија преварних радњи се ипак издваја као доста специфична. Пре свега, код превара је ревизија по правилу реактивна, посебно тамо где *Fraud Management* не постоји. Иако постоји могућност да се превентивно делује, на пример давањем препорука за унапређење контрола, ипак у већини случајева ревизија делује детективно или само реактивно – тек по насталом инциденту. Обично се такве ревизије врше по ванредном радном налогу и имају несистемски карактер, карактер једнократне провере или истраге.

Када је у случајеве преваре укључена технолошка компонента, може се појавити и потреба за применом дигиталне форензике. Треба имати у виду да је примена дигиталне форензике у корпоративном окружењу битно различита од оне која постоји код истражних и судских органа. Та разлика се пре свега читава у природи и тежини учињеног дела, што се онда одражава и на мотивацију и обим форензичких захвата. Корпоративна форензика је применљива искључиво онда када је потпуно јасно да преварна радња спада у категорију која се санкционише искључиво интерним актима (нема елементе кривичног дела и сл) и када њене последице ни у ком аспектима не излазе из оквира компаније.

Ова област је веома осетљива и мора бити третирана са посебном пажњом. Никако се не сме дозволити да се интерна ревизија упушта у било какву истрагу преваре или примену дигиталне форензике без експлицитног и прецизног налога од стране овлашћеног руководиоца и уколико у свом саставу нема одговарајуће обучене и увежбане специјалисте са свим потребним знањима и искуством за обављање таквих задатака.

2.6.3. Ревизија усклађености

Ревизија усклађености (*Compliance Audit*) у ширем смислу односи се на ревизију нормативне усклађености, тј на давање мишљења и оцене у погледу поштовања сваке врсте регулативе. Ту пре свега спадају закони, затим стандарди, стручна и професионална регулатива, интерна акта (политике, правилници, процедуре) итд.

У контексту технолошке ревизије, под ревизијом усклађености се пре свега подразумева ревизија која утврђује да ли организација испуњава норме прописане неким конкретним стандардом. Ова врста ревизије се понекад назива и сертификациона ревизија, јер организација која при оваквој ревизији буде позитивно оцењена добија одговарајући сертификат о усклађености. Њу обављају посебни, овлашћени ревизори, специјализовани за сваки одређени стандард, по процедурама које су строго дефинисане

и формализоване. Неки примери ревизије усклађености су: *ISO 9000*, *ISO 27001*, *Sarbanes-Oxley (SOX 302, SOX 404)*, *Basel II*, *PCI DSS*, *ISO 15408 – Common Criteria* итд.

2.6.4. Самооцењивање

Самооцењивање је врста ревизије код које сви нивои управе заједно са запосленима (руководством и оперативним особљем) учествују у процени ризика и њима припадајућих контрола у организацији. Изворни назив за ову врсту ревизије је *Control Risk Self-assessment (CRSA)*. Она се изводи посебним техникама и алатима, обично у тзв „радионицама” (*CRSA Workshops*), којима руководе посебно обучени (најчешће технолошки) ревизори.

У основи самооцењивања је идеја да се, у циљу откривања слабости, уместо уобичајених провера и тестова које ревизори врше током рада на терену, организује радионица у којој би изванредан број плански изабраних учесника предметног пословног процеса био у прилици да слободно изнесе сопствену оцену о предмету ревизије.

Тако на пример, уместо да се до ревизорског налаза долази кроз разговор са шефом неке службе, у радионицу се позову сви радници те службе и омогући им се да лично изнесу сопствене налазе. Претпоставка од које се полази јесте да у великом броју случајева запослени најбоље познају слабости система у којем раде, али да се ретко одлучују да то изнесу у разговору са трећим лицима, посебно са ревизорима.

Да би оваква техника била објективна и дала аутентичан резултат, неопходно је остварити низ предуслова. Пре свега, потребно је постићи поуздан ниво анонимности учесника. То се најчешће постиже коришћењем уређаја за анонимно гласање, попут оних у парламентарним дворанама, само мањих и прилагођених потребама оваквих радионица. Ти уређаји су обично преносиви, чиме се омогућава да се радионице организују у непосредној близини радних места учесника. Такође, неопходна је посебна обука за водитеље (помагаче - *facilitators*) тих радионица, будући да они морају имати посебна знања и вештине из разних домена (техничка, социјална итд). Од посебне важности је процес планирања и припреме у којем се доносе одлуке о избору учесника, списку питања која ће бити постављена итд. Питања морају бити постављена тако да се одговори дају избором вишеструких опција (тзв тест питања, где се одговори дају избором – *a, b, c* или *g*). Учесник даје одговор притиском на тастер а резултати су потпуно деперсонализовани и одмах се статистички обрађују. Обрада се најчешће врши у реалном времену, на лицу места, тако да учесници имају могућност да се одмах упознају са резултатима. На крају, али вероватно најважније, јесте да је за овакав рад неопходна врло јака подршка од стране руководства.

Ова врста ревизије има многе недостатке који је чине неприменљивом у многим ситуацијама. Јасно је да се самооцењивање не може применити у ситуацијама где се ради о оцени веома високих пословних ризика, или за истраживање превара, случајева корупције и слично. Такође, ако корпоративна култура није одговарајућа, учесници радионица неће никада давати искрене одговоре, па чак ни на најбезазленија питања. Међутим, у великом броју примена се показало да се оваквим приступом могу остварити велике уштеде у броју и радном времену ревизора, као и у поузданости и општој вредности ревизорских резултата. Неке од области у којима се показало да самооцењивање може да буде врло успешно су: ревизија развојних пројеката система и

апликација, рада оперативних центара за надзор технолошке инфраструктуре, позивних и услужних центара за бригу о корисницима, оцена познавања разних процедура и увежбаности њихове примене (на пример реаговање на инциденте и сл), оцена квалитета корисничке документације, прихватљивости апликација од стране корисника итд

2.7. РЕВИЗОРСКИ АЛАТИ

2.7.1. *Општи ревизорски алати – рачунарска подршка ревизији*

Већ од првих дана појаве рачунарске технике у рачуноводству јавила се идеја о развоју посебних софтверских алата који би пружали подршку ревизорима у обављању свакодневних задатака. Први софтверски производи ове врсте називани су заједничким именом општи (генерализовани) ревизорски софтвер (*GAS – Generalized Audit Software*). Касније, са развојем рачунарске технике и информационих технологија ова област се развила до препознатљивости која је издваја у потпуно засебну категорију. Назив који се данас најчешће користи је „алати (и технике) за рачунарску подршку ревизији” (*CAATT – Computer Aided Audit Techniques and Tools*, понегде кратко *CAAT – Computer Aided Audit Tools*). Већина актуелних производа усмерена је на што бржу обраду велике количине података. Статистичке анализе, корелације, сортирања, поређења и многе друге операције над великим скуповима бројева као и израда свих врста извештаја у овим програмима се обављају знатно ефикасније него у генеричким програмима за обраду табела (*spreadsheet*), програмима за управљање базама података на персоналним рачунарима (*MS Access* и сл.) или у програмима за форматирање извештаја (*Crystal Reports* и други). У даљем тексту даје се преглед најважнијих представника ове категорије софтвера.

а) **ACL**

Овај алат, производ истоимене фирме (*ACL – Audit Command Language*), већ дуже време је водећи софтверски пакет за рачунарску подршку ревизији. Он је у стању да врши анализе врло великих скупова података, тако да ревизори не морају да узимају статистичке узорке, већ им је омогућено да раде на целокупној популацији. Овим алатом могуће је анализирати трендове, идентификовати изузетке, открити грешке у подацима или индикаторе потенцијалних преварних радњи и генерисати веома разноврсне и квалитетне извештаје. Аналитичарима стоје на располагању веома бројне математичке, статистичке, финансијске, рачуноводствене и друге функције које се могу аутоматизовати у сложене аналитичке задатке, помоћу уграђеног скрипт језика и припадајућег језичког интерпретатора. Подаци се преузимају директно из базе података, формирањем одговарајућих *SQL* упита. Приступ је сигуран, без могућности модификације (*read-only*), а све операције одвијају се на верној копији изворних података (*image – слика, одраз*).

б) **IDEA (CaseWare IDEA Inc.)**

Назив овог алата је скраћеница, са значењем „интерактивно издвајање и анализа података” (*IDEA – Interactive Data Extraction and Analysis*). Намена и могућности овог алата су слични претходном, с тим да постоје значајне разлике у имплементацији и коришћеним технологијама. На пример, приступ базама података код програма *ACL* је

решен преко SQL упита, док се у програму *IDEA* користе упити у језику *VBA (Visual Basic for Applications)*, врло слично приступу који имају *MS Excel* и остали програми из пакета *MS Office*. Према већини функција које поседује и укупним перформансама, *IDEA* је главни конкурент програму *ACL* на тржишту ревизорског софтвера.

в) Reliant Auditor (*Reliant Solutions, Inc.*)

Док су *ACL* и *IDEA* усмерене на помоћ ревизору који непосредно извршава ревизорски задатак, *Reliant Auditor* је усмерен на помоћ руководиоцима – менаџерима који управљају процесима ревизије. Овај алат помаже у планирању ревизије (израда годишњег плана и програма појединачних ревизорских задатака), тестирању и проценама контрола и праћењу примене препоручених мера (*Follow-up*). Такође, он има уграђене функције за континуирано праћење система интерних контрола, евидентирање ревизорских извештаја, радних папира и друге релевантне документације.

г) TopCAATs (*Reinvent Data Ltd*)

За разлику од претходних (*ACL*, *IDEA* и *Reliant*), који се истичу снагом и сложености, тежиште алата *TopCAATs* је на једноставности употребе и на ниској цени. Овај алат заправо и није самосталан програм, већ је реализован као додатак (*plug-in*) за постојеће програме из пакета *MS Office* (на пример *MS Excel*). Пакет *TopCAATs* додаје велики број специјализованих ревизорских функција на већ постојећи скуп функција програма *MS Excel*, тако да се од обичног програма за обраду табела добија врло функционалан алат за подршку ревизорским активностима.

д) ActiveData (*InformationActive*)

По својим могућностима и начину реализације, овај алат је врло сличан претходном (*TopCAATs*). То је такође додатак за *MS Office*, који уводи низ нових функција у програме за рад са табелама и за обраду текста. На тај начин се један стандардни канцеларијски пакет оспособљава за специфичне ревизорске задатке – анализу података, писање извештаја итд. Програм *ActiveData* се истиче једноставношћу инсталације и употребе, као и релативно ниском ценом.

ђ) Monarch Professional (*Datawatch*)

Овај производ није намењен искључиво ревизорима, али може да буде од велике користи у њиховом раду. Изворна намена овог програма јесте претраживање и корелисање слободно форматираних података у циљу проналажења одређених веза, правила и садржаја који нам могу бити од интереса. Категорија којој овај програм припада је релативно нова – то је област вођења тзв „пословних истрага” (*Business Intelligence*). Такође, технологија „копања по подацима” (*Data Mining*), на којој се овај програм заснива, припада генерацијски новијим технологијама. У примеру овог програма, ова технологија омогућава претраживање не само по нумеричким и табеларно сређеним подацима (попут оних у базама података), већ и врло ефикасно претраживање по слободно или слабо форматираном тексту у документима најразличитијих типова, као што су: *TXT*, *PDF*, *XPS*, *XLS*, *CST/CDT*, *HTML*, *XML* и други.

е) Програми за опште статистичке намене

Иако им нису посебно намењени, статистички програми општег типа, као што су SAS (*Statistical Analysis System*) и SPSS (*Statistical Package for Social Sciences*) могу да буду од велике помоћи ревизорима. Уколико организација већ поседује неки од ових програма (или неки други сличан софтвер) онда је препоручљиво и исплативо искористити ту (већ постојећу) инвестицију и омогућити ревизорима да ове програме искористе за своје потребе.

2.7.2. Специјализовани ревизорски алати – рачунарска подршка технолошкој ревизији

За разлику од претходне групе алата, који су настали као регуларни одговор софтверске индустрије на захтеве и исказане потребе одређене професионалне корисничке групе, већина алата у овој групи настала је као резултат рада индивидуалних професионалаца у настојању да реше неки од сопствених проблема, да докажу исправност неке претпоставке или остваривост неке идеје. Они су углавном започети као неки мали и уско специјализовани хакерски експеримент. Неки су то и до данас остали, док се један број развио до нивоа веома зрелих и поузданих софтверских производа. Иако су неки од њих касније и комерцијализовани, највећи број је остао и даље јавно доступан и бесплатан. Употребљивост и перформансе ових програма варирају у великој мери, али је избор огроман, тако да је сасвим сигурно да се за сваки специфичан задатак из области технолошке ревизије може наћи одговарајући, веома користан програм за неку од следећих примена.

а) Мапирање мрежа

У ову групу алата спадају програми за идентификацију активних рачунара и мрежних уређаја, програми за идентификацију отворених портова (*Port Scanners*), програми за идентификацију оперативних система и сервиса (*Fingerprinting*) и скенери виртуелних приватних мрежа.

Најпознатији представник ове групе је програм по имену **nmap**. То је иначе бесплатан програм који се налази у јавном домену (лиценциран је по GPL лиценци) аутора познатог по псеудониму „Фјодор“ (*Fyodor*, <http://www.insecure.org>). Иако се програмом **nmap** могу успешно обавити практично све операције на мапирању мрежа (и више од тога), ипак је потребно поменути и неколико из мноштва осталих програма који се такође користе, како за неке специфичне задатке тако и за контролу резултата добијених програмом **nmap**.

За откривање активних мрежних адреса то су **ping**, **fping**, **hping2/3**, **thc-rut**, **5NMP** и **nbtscan**. За скенирање портова користе се **NSAT**, **netcat**, **autoscan** и **superscan**. За идентификовање оперативних система, апликација и сервиса користе се **amap**, **xprobe2**, **protos**, **p0f**, а за анализу виртуелних приватних мрежа **ike-scan** и **psk-crack**.

б) Анализа бежичних мрежа

Већину савремених бежичних мрежа чине мреже засноване на стандарду *IEEE 802.11* (WiFi, WLAN). Овај стандард омогућава једноставно и економично повезивање рачунара у локалне мреже ограниченог домета и брзине. Упркос многим недостацима, постао је веома популаран и широко примењен, пре свега у локалним рачунарским мрежама мањих и економски слабијих организација и у мрежама за приступ Интернету. Поред овог стандарда, у широкој примени, али са врло специфичним наменама, су још и *Bluetooth* (PAN – *Personal Area Networks*) и *RFID* (*Radio-frequency identification*) технологије. Од ова три стандарда, *IEEE 802.11* је најчешћи предмет технолошке ревизије, пошто су грешке у конфигурацији доста честе и могу да имају значајне безбедносне импликације. За *Bluetooth* и *RFID* уочљив је пораст интересовања међу технолошким ревизорима, али је заостатак у погледу алата још увек доста велики. Бежичне технологије са применом у телекомуникацијама и WAN мрежама (*GSM*, *GPRS*, *UMTS*, *WiMax*, *DECT*, *CDMA* итд) још увек се ретко подвргавају ревизорским анализама.

Најпознатији алати за анализу *IEEE 802.11* су **kismet**, **netstumbler** (детектори, прислушкивачи саобраћаја) и **aircrack-ng** (разбијање WEP и WPA-PSK шифарских кључева).

За анализу *Bluetooth* протокола ревизорски алати су још увек несавршени и недовољно функционални. Из мноштва програма, који су углавном хакерског типа, издвајају се **btscanner** и **blueprint** (идентификација и скупљање података о уређајима без претходног захтева за упаривање).

Технологија за радиофреквентну идентификацију (*RFID*) је постала предмет интересовања технолошке ревизије тек недавно. За сада, једини иоле употребљив скуп алата за ревизију ове технологије јесте тзв **RFIDiot**.

в) Идентификовање слабости система

Постоји велики број комерцијално доступних скенера за откривање системских слабости. Најпознатији су *ISS Internet Scanner*, *eEye Retina*, *GFI LanGuard*, *Qualis Vulnerability Scanner*, итд. Међу њима се истиче **Nessus**, програм који је годинама био јавно доступан и бесплатан, а који је од недавно прешао у комерцијалну понуду фирме *Tenable Soft*. Једна верзија овог програма, уз незнатна ограничења, још увек је бесплатна. Огромна популарност овог софтвера долази од препознатог квалитета, поузданости резултата и високих перформанси, захваљујући којима овај програм успешно конкурише и знатно скупљим програмима великих произвођача.

г) Ескалација привилегија

У овој групи се налазе програми за погађање и откривање лозинки (*password guessing/cracking*), за прислушкивање и анализу мрежног саобраћаја (*sniffing*) и за конструисање и подметање нерегуларних пакета у регуларни мрежни саобраћај (*spoofing*).

Водећи алати за „разбијање” лозинки су **john (the ripper)**, **bkhive**, **cain&abel**,

samdump2 и **rainbowcrack**. Поред „разбијања”, које се по правилу врши *off-line*, уз помоћ речника и именика, лозинке се могу погађати и „уживо” (*on-line*), применом комбинаторике (*brute force*) или речника/именика. За те потребе служе програми као што су **thc-hydra**, **bruteSSH** или **medusa**.

Водећи програми за анализу саобраћаја су **wireshark**, **tcpdump**, **ethercap**, **dsniff** и **snort**.

Најпознатији алати за „фалсификовање” саобраћаја (*spoofing*) су **etherape**, **ethercap**, **scapy** и **tcpreplay**.

д) Пробојни тестови

За аутоматизацију пробојних тестова (*penetration testing*) најпознатији и најчешће коришћени алат је *Metasploit Framework*. Иако је бесплатан и доступан у јавном домену, овај алат снажно конкурише комерцијалним производима исте намене као што су *Immunity Canvas* и *Core Impact*. Овде треба поменути и програм **inguma**, који је уско усмерен на пробојне тестове *Oracle* база података.

ђ) Анализа трослојних апликација

За ревизију база података, поред комерцијалних, као што су *AppDetective* и *ISS Database Scanner*, често се користе и бесплатни, јавно доступни алати, као што су **mssqlscan**, **mysqldaudit**, **oscanner** и други.

За ревизију апликационих сервера и веб апликација постоје многа комерцијална решења, као што су *WebInspect* (раније *SPIDynamic*, сада *HP*) и *Acunetix*. У јавном домену, најпознатији су **burp**, **webscarab**, **nikto** и **paros proxy**.

е) Анализа ИП телефоније (VoIP)

Саобраћај ИП телефоније може бити сниман и анализиран алатима који генерално служе снимању и анализи ИП саобраћаја. Међутим, постоји низ алата који „разумеју” *SIP* протокол и који могу да манипулишу *VoIP* на нивоу телефонске сигнализације (успостава и раскидање везе), на нивоу телефонског разговора (прислушкивање, снимање и репродукција) итд. Најпознатији алати у овој групи су **sipscan**, **sipdump/sipcrack**, **sipvicious**, **protos-sip**, **voiper** и **vomit**.

ж) Дигитална форензика

Примена дигиталне форензике у технолошкој ревизији се значајно разликује од примене у криминалистици и судским истражним поступцима. Технолошким ревизорима најчешће нису неопходни високо професионални алати (*EnCase* и сл.), већ своје задатке могу да обаве и коришћењем далеко једноставнијих и јефтинијих, па чак и бесплатних алата. За форензичко копирање медијума (*imaging*) користе се **dcfldd**, **dd**, **aff** и **aimage**, док се за форензичку анализу користе **autopsy**, **foremost** и **scalpel**.

Треба напоменути да је, због специфичности поступака у дигиталној форензици, врло

чест случај да се формирају збирке неопходних алата у облику тзв „живих” (bootable) CD или DVD дискова. На овим дисковима налазе се комплетни оперативни системи, који се покрећу независно од система који се форензички испитује. На тај начин је могуће обавити велики број форензичких активности, без измена или оштећења предметног система. Неки од истакнутијих примера су *helix3*, *deft linux*, *fscsi 4n6* итд.

з) Пакети и дистрибуције

Слично збиркама алата за дигиталну форензику, на CD или DVD медијумима се често дистрибуирају збирке одабраних алата за послове технолошке ревизије, ревизије информатичке безбедности, пробојних тестова и слично. Најпознатији примери оваквих дистрибуција су *BackTrack* (пробојни тестови) и *OWASP LiveCD* (тестирање веб апликација).

2.8. ПРОФЕСИОНАЛНА КОМПЕТЕНЦИЈА ТЕХНОЛОШКИХ РЕВИЗОРА

Компетентност је један од четири принципа којих се, према Етичком кодексу, ревизори морају придржавати. Овај принцип налаже интерним ревизорима да морају да примењују сво знање, вештине и искуство које је неопходно за вршење интерне ревизије. У циљу поштовања принципа компетентности, интерни ревизори се, поред осталог, обавезују и да ће узимати учешћа само у оним активностима за које поседују неопходна знања, вештине и искуство, као и да ће непрекидно радити на усавршавању својих знања и вештина. Непрекидно професионално усавршавање прописује и Стандард 1230, док Стандард 1210 налаже ревизорима (и интерној ревизији као целини) да „морају имати знања, вештине и остале компетенције неопходне за спровођење личних одговорности”.

Обим знања, вештина и других компетенција које морају да поседују технолошки ревизори је веома широк и обухвата не само стручна, техничка и друга ревизорска знања и вештине, већ и знатно више од тога.

2.8.1. Техничка знања

Технолошки ревизори пре свега треба добро да познају област технологије чијом ревизијом се баве. То знање мора да буде довољно за правилно и потпуно разумевање предмета ревизије. Оно не мора да буде у рангу знања оних професионалаца (специјалиста) који се непосредно баве том конкретном облашћу технологије, али мора да има здраве основе, јасну и уређену структуру и да буде довољно за извођење правилних закључака и доношење правилних оцена.

Технолошки ревизори морају одлично познавати стандарде, смернице, препоруке и другу професионалну регулативу која се односи на област технолошке ревизије.

Технолошки ревизори морају имати довољне вештине за рад на различитим платформама (оперативним системима и техничким уређајима), различитим софтверским апликацијама, за приступ, екстракцију и анализу информација из база података и друге вештине које им омогућавају да се у технолошким окружењима сналазе са лакоћом и раде самостално или у тиму.

Поседовање најширег знања у што већем броју технолошких области је свакако пожељно, као што је и поседовање детаљних (специјалистичких) знања у неким од њих. Међутим, вероватно је од свега најважније поседовање спремности за стално усавршавање и учење, и непрекидно исказивање интересовања за сва питања из области информacionих и комуникационих технологија.

2.8.2. Општа пословна и ревизорска знања

Технолошки ревизори морају да поседују детаљна и поуздана знања о пословању организације којој припадају. Ту пре свега спадају стратешки и други пословни циљеви, организациона структура, пословни процеси и припадајућа подела улога и одговорности итд.

Технолошки ревизори морају одлично познавати Стандарде интерне ревизије, познавати Етички кодекс (и придржавати га се), стално пратити развој ревизорске теорије и праксе и усвајати нова сазнања из области интерне ревизије.

Иако су превасходно окренути технологији, за технолошке ревизоре је веома пожељно да стекну основна знања и из области финансија, рачуноводства и опште економије. Не очекује се подробна едукација и увежбавање, али је веома корисно ако технолошки ревизор има разумевање и познавање основних појмова у мери која му омогућава успешну тимску сарадњу са финансијским ревизорима. Исто важи и за знања из области права и регулативе, као и за област менаџмента.

2.8.3. Социјалне вештине и способности

Поред стручних знања из области технологије, пословања и опште ревизије, технолошки ревизори морају поседовати и низ других вештина које им олакшавају рад са клијентима, рад са тимским колегама и генерално доприносе њиховој успешности у ревизорским активностима.

Ревизори ретко раде сами. Они су обично део тима. Успех сваког тимског рада зависи у великој мери од личних особина појединих чланова. За технолошког ревизора је веома битна способност да ради у тимском окружењу – прилагодљивост природи других индивидуа, комуникативност, отвореност, опхођење с поштовањем, прихватање ауторитета и лидерства вође тима, прихватање равноправности других чланова итд. Иако се на већину набројаног обично гледа као на особине личности, које су део природе појединца и не могу се мењати, веома је важно за сваког ревизора да ту перцепцију коригује и прихвати да су све то заправо знања и вештине, попут других – једноставно, то су способности које се могу стећи и усавршавати учењем.

Поседовање ових вештина је од посебног значаја у односима са клијентом ревизије. Један од најзначајнијих фактора успеха ревизије је у томе да клијент стекне уверење да су он и ревизори заправо чланови истог тима и да раде на истом задатку. Ревизор мора имати способност да превлада природни отпор који према ревизији постоји код сваког клијента. Знања и вештине из области техника убеђивања, техника презентације, познавање „говора тела”, психологије људског понашања итд су у том погледу такође врло пожељна.

Поред тога, веома пожељне су и способности и вештине артикулације. Јасно, концизно и убедљиво изражавање је од огромне користи – не само вербално – на састанцима са колегама и клијентима, већ и у писаној форми – приликом израде писаних извештаја.

2.8.4. Перманентна едукација и професионална сертификација

Интерни ревизори се морају подстицати да степен своје стручне усавершености непрекидно подижу – праћењем стручне литературе и периодичних публикација у штампи или на Интернету, похађањем семинара, стручних скупова и конференција, учествовањем у *on-line* форумима итд.

Потреба за сталним усавршавањем је у области технолошке ревизије посебно изражена због врло брзог и интензивног развоја савремених технологија. Данас већина технолошких знања застарева већ након три до четири године, тако да за сваког технолошког ревизора питање перманентне едукације постаје кључно питање у његовој каријери – питање професионалног опстанка.

Због тога је веома пожељно да се стечена знања стално проверавају и доказују кроз неки од признатих сертификационих програма, специјализованих за метрику стручних компетенција. У тим програмима се, полагањем стручних испита, стичу одговарајући професионални сертификати, као објективан доказ демонстрираних стручних компетенција.

Преглед неких значајнијих професионалних сертификата из области опште и технолошке ревизије и информатичке сигурности дат је у прилогу 4.4.

2.9. ПРОФЕСИОНАЛНА РЕГУЛАТИВА – СТАНДАРДИ, ПРЕПОРУКЕ И РАДНИ ОКВИРИ

2.9.1. Стандарди Института интерних ревизора

Институт интерних ревизора (*The Institute of Internal Auditors – IIA*), као највећа професионална организација у области интерне ревизије, развио је сопствене стандарде за професионално обављање интерне ревизије и то као засебни део тзв „Оквира за професионалну праксу” (*Professional Practices Framework*). Овај оквир састоји се од три дела:

- Дефиниција интерне ревизије (видети тачку 2.2.1. *Дефиниција интерне ревизије*)
- Етички кодекс (видети тачку 2.2.3. *Професионална етика*)
- Међународни стандарди за професионалну праксу интерне ревизије

Ови стандарди, под називом „Међународни стандарди за професионалну праксу интерне ревизије” (*International Standards for the Professional Practice of Internal Auditing*) данас су прихваћени од стране стручне јавности целог света и усвојени као (*de-facto*) стандарди и извор основних смерница за читаву професију.

Овај документ је по својој структури подељен на три дела. Први део представљају

такозвани Стандарди својстава (*Attribute Standards*) а други су Стандарди учинка (*Performance Standards*). Трећи део је Речник (појмовник) у коме су објашњени основни термини и дефинисани појмови који се у Стандардима користе

Стандарди својстава утврђују основне карактеристике интерне ревизије, односно организационе целине која обавља ту функцију. У њима се утврђују сврха, циљеви и основни предуслови за постизање објективности, независности и компетентности интерне ревизије као и њена улога и одговорности.

Стандарди учинка утврђују критеријуме по којима је могуће мерити учинак интерне ревизије. Ови стандарди постављају основе за организовање, планирање и извођење ревизије, као и за процесе извештавања и праћења реализације препоручених мера у оквиру организационе јединице која обавља интерну ревизију.

Стандарди својстава и Стандарди учинка односе се подједнако на саветодавне активности интерне ревизије као и на активности на пружању уверења. Поједини стандарди из обе групе стандарда праћени су нешто детаљнијим упутствима, која су у ранијим верзијама (до 2004. године) носила назив Имплементациони стандарди. У новијим верзијама Међународних стандарда (2008. и 2009.), ова упутства су задржана, али без посебног назива.

Потребно је нагласити да се ови стандарди односе на интерну ревизију у целини и то у најопштијем смислу. У њима нема посебних референци на специјализоване облике ревизије, па се тако у њима не може наћи ништа што би се посебно односило на поступке и праксу технолошке ревизије. Информациони системи се помињу дословце на само два места у тексту документа, без икаквог посебног разматрања ове области.

Институт интерних ревизора у новије време посвећује пажњу ревизији технологија и то кроз две посебне серије публикација, под ознакама *GTAG* и *GAIT*. Прва серија (*GTAG – Global Technology Audit Guides*) покрива основна упутства за ревизију технологија, док је друга (*Guide to the Assessment of IT Risk – GAIT*) тематски усмерена на давање упутстава за процену ризика који потичу од примене технологија. Листа наслова који су до данас објављени у ове две серије публикација дата је у Прилогу 4.2.

2.9.2. Стандарди Асоцијације за ревизију и контролу информационих система (Information Systems Audit and Control Association – ISACA)

Асоцијација *ISACA* је успоставила своје оквире за ревизију информационих система, који се састоје из два дела. Први део су „Стандарди, смернице, алати и технике за професионалце у области ревизије, давања уверења и контроле информационих система” (*IS Standards, Guidelines and Tools and Techniques for Auditing and Assurance and Control Professionals*), док је други представљен у публикацији под називом „Управљачке смернице за информационе и сродне технологије” (*COBIT – Control Objectives for Information and Related Technologies*).

а) Стандарди

Структура „Стандарда, смерница, алата и техника за професионалце у области ревизије, давања уверења и контроле информационих система” је сложена и састоји се из три

главна дела:

- Кодекс професионалне етике за ревизоре информационих система
- Стандарди, упутства, алати и технике за ревизију и давање уверења у области ИТ
- Стандарди за управљање (контролу) ИС.

Кодекс професионалне етике и Стандарди дефинишу обавезујуће захтеве за ревизију информационих система. Они имају значај за ревизоре информационих технологија, руководство у организацијама као и за чланове Асоцијације *ISACA* (посебно за власнике сертификата *CISA/CISM*). За ревизоре, они постављају минималне захтеве у погледу ревизорског учинка. За менаџере, они дају информацију о очекивањима која се могу поставити пред извршиоце ревизорских задатака, док за сертификоване професионалце и чланове *ISACA*, они имају снагу закона чије се кршење санкционише дисциплинским мерама Асоцијације. Треба напоменути да је Кодекс професионалне етике у потпуности у складу и у највећој мери подударан са Етичким кодексом *IIA*, тако да овде неће бити потребно посебно излагати његове одредбе.

Помоћ у тумачењу и примени Стандарда дата је у посебном делу („Упутства”). Ту се ревизор информационих система упућује на који начин да приђе имплементацији Стандарда, како да професионално просуђује о њиховој примени, односно како да врши процену евентуалних одступања у односу на њих. Сврха „Упутстава” је да пружи детаљне информације о томе како се постиже пуна усклађеност са стандардима.

У делу „Алати и технике” дају се конкретни примери процедура по којима ревизор информационих система може да приступи појединим ревизорским задацима. Врло детаљно, у обиму од око стотинак страница, покривено је укупно једанест примера, који се сусрећу у пракси ревизора информационих система. Ту су, између осталог, процедуре за процену и мерење ризика у ИС, процедуре за ревизију система за детекцију упада (*IDS*), мрежних баријера (заклона, запрека – *firewalls*), антивирусних решења, шифровања података, електронског потписивања, инфраструктуре јавних кључева итд.

б) Управљачке смернице

КОБИТ (*COBIT – Control Objectives for Information and Related Technologies*) представља најдетаљније разрађене радне оквири за област ревизије и управљања информационим технологијама који се данас могу наћи на тржишту. Овај обимни документ је најважнији производ у понуди асоцијације *ISACA*. У њему је сабрана најбоља професионална пракса у области ревизије и управљања савременим технологијама.

Његова структура је следећа:

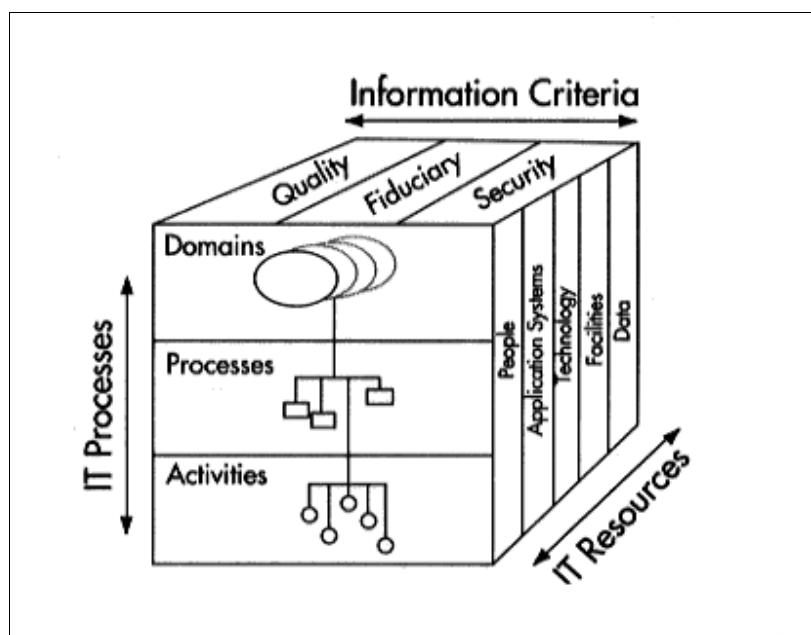
- Кратак преглед (*Executive Summary*)
- Управљачко – контролни оквир (*Governance and Control Framework*)
- Упутства за руководиоце (*Management Guidelines*)
- Управљачке смернице (*Control Objectives*)
- Управљачка пракса (*Control Practices – Implementation Guide*)
- Упутства за ревизоре (*Audit Guidelines – IT Assurance Guide*)

У области управљања технологијама КОБИТ препознаје 34 процеса, које сврстава у 4 домена. Ти домени су:

- Планирање и организација (*Planning and Organization*)
- Набавка и имплементација (*Acquire and Implementation*)
- Испорука и подршка (*Deliver and Support*)
- Праћење и оцењивање (*Monitor and Evaluation*)

Уочљиво је да подела на домене одговара животном циклусу технолошких система у организацијама где се они примењују. Сваки од 34 процеса праћен је одговарајућим управљачким смерницама, посебно за менаџмент а посебно за оперативну праксу. Листа процеса и њихова подела по доменима дата је у Прилогу 4.2.

Иначе, карактеристични приступ који се у КОБИТу користи најчешће се илуструје тродимензионалним приказом, тзв „коцком” (*COBIT Cube*), која је дата на Слици 4.



Слика 4: Три димензије CobiT приступа

Прву димензију коцке чине пословни захтеви у погледу квалитета, безбедности и усклађености. Захтеви у погледу квалитета се односе на квалитет у ужем смислу, цену и испоруку (благовремену, комплетну итд). Захтеви безбедности се односе на тајност, интегритет и расположивост. Легална усклађеност (*Fiduciary*) се односи на захтеве из COSO извештаја – оперативна ефективност и ефикасност, поузданост информација и усклађеност са законима и регулативом (*Effectiveness and Efficiency of Operations, Reliability of Information, Compliance with Laws and Regulations*). Након анализе, ови захтеви се могу свести на седам основних информационих критеријума: ефективност, ефикасност, расположивост, интегритет, тајност, поузданост и усклађеност.

Друга димензија обухвата све врсте ресурса значајних за ову област. Ту спадају: подаци, физички објекти, технологија, апликације и људство. Физички објекти и технологија често се приказани заједно, под називом инфраструктура.

Трећа димензија обухвата три слоја. Први слој су четири већ поменута домена (*PO, AI, DS, ME*). Други слој обухвата препознате процесе у сваком од домена (укупно 34

процеса), док у трећем слоју имамо још детаљнију декомпозицију, где се налазе детаљне управљачко – контролне активности унутар сваког процеса (укупно 318 контролних смерница).

КОБИТ је посебно значајан за технолошке ревизоре, пошто је један његов део посвећен искључиво упутствима за вршење технолошке ревизије. У том делу, за сваки од процеса дају се упутства за мерење и оцењивање практичне усклађености са задатим управљачким оквиром. Конкретно, смернице за контролу и мерење резултата, КОБИТ организује у четири целине, које су посебно дефинисане за сваки од 34 процеса:

- **Модел за процену зрелости** (*Maturity Model*), који помаже организацији да упореди своје стање или свој напредак са најбољим примерима препознатим у датој области или са циљевима које она жели да постигне
- **Критични чиниоци успеха** (*Critical Success Factors*), у којима се дефинишу најважније претпоставке које морају бити испуњене од стране руководства да би се омогућило постизање одређених пословних циљева
- **Кључни показатељи циљева** (*Key Goal Indicators*), као мерне вредности које показују степен остварености постављених циљева (мерење на крају процеса)
- **Кључни показатељи учинка** (*Key Performance Indicators*), као мерне вредности које показују колико повољно се један процес одвија у смеру коначног постизања постављених циљева (мерење у току процеса).

Модел за процену зрелости утврђује шест нивоа развоја за сваки идентификовани процес, који се могу користити за оцену стања развоја у којем се предметни процес налази:

(0) Не постоји (*Non existent*). За процес се може дати оцена да не постоји уколико у организацији уопште није препозната потреба да се дати процес издвоји као засебан и да се за њега успоставе посебне управљачко-контролне мере.

(1) Иницијално / ад-хок стање (*Initial/Ad Hoc*). Ова оцена се даје процесу који је препознат, али за њега нису успостављене посебне управљачко-контролне мере. У случају да се појави тренутна потреба, примењују се мере управљања и контроле, али се оне креирају једнократно и на бази конкретног, појединачног случаја. Приступ је у потпуности реактиван, без посебног плана и припреме. За сваки поновљени случај, приступ се креира поново, а решења се проналазе „од случаја до случаја”, дакле импровизовано.

(2) Поновљиво, али интуитивно стање (*Repeatable but Intuitive*). Ову оцену добијају процеси који су препознати и који су се усталили, али нису уједначени и документовани на нивоу целе организације. Они се регуларно одвијају, али на основу индивидуалних одлука које доносе поједини руководиоци. Ризици од ових одлука или евентуална корист од њих препуштени су руководиоцевој интуицији. Ток и резултати процеса разликују се у зависности од индивидуалних знања и способности појединаца који управљају процесом.

(3) Дефинисано стање (*Defined*). За процес се каже да је дефинисан ако постоји нека пословна одлука (политика, процедура и сл.) којом се прописује приступ

управљању и одвијању тог процеса. Начин одвијања процеса је документован и саопштен свим релевантним факторима у организацији. Међутим, обука за прописани поступак није конзистентно спроведена, нити постоје контролне мере које обезбеђују да се процес заиста мора одвијати на прописани начин.

(4) Управљано и мерљиво стање (*Managed and Measurable*). Процес у стању управљаности и мерљивости је напреднији од процеса у стању дефиниције утолико што не само да постоји прописани, документован и саопштен начин његовог одвијања, већ су успостављене и мере за проверу његовог тока и за оцењивање постигнутих резултата и учинка, односно испуњења очекиваних циљева. Процеси се прате (*Monitoring*), линије одговорности су успостављене, а извештавање по тим линијама одговорности је редовно. Постоји начин реаговања у случају да се установи одступање. Аутоматски алати се при томе користе ограничено или фрагментарно.

(5) Оптимизовано стање (*Optimized*). Најбоља пракса је успостављена и сасвим аутоматизована. Процеси су усавршени као резултат сталног унапређивања и примене најбољих примера праксе из других организација. ИТ се користе на интегрисан начин за аутоматизацију свих радних процеса, што представља средство за побољшање квалитета и ефективности и доприноси брзој прилагодљивости организације свим променама.

Будући да обезбеђује незаменљиве инструменте за контролу, управљање, праћење, мерење резултата и ревизију у области примене савремених технологија, КОБИТ се наметнуо као референтни радни оквир и стандард за све професионалце у овој области.

2.9.3. Стандарди COSO

КОСО (*COSO – Committee Of Sponsoring Organizations of Treadway Commission*) је тело формирано 1985. године од стране пет водећих америчких организација у области рачуноводства и ревизије (тзв „спонзора“) ради пружања стручне помоћи тзв Тредвејевој комисији у области контроле над финансијским извештајима и спречавања злоупотреба и превара у рачуноводству. Тредвејева комисија је добила име по свом првом председнику (*James C. Treadway*). Њен прави назив је *National Commission on Fraudulent Financial Reporting*, а спонзори и оснивачи су били:

- *American Institute of Certified Public Accountants (AICPA)*,
- *American Accounting Association (AAA)*,
- *Financial Executives International (FEI)*,
- *Institute of Internal Auditors (IIA)* и
- *Institute of Management Accountants (IMA)*.

а) Оквир за интерну контролу и управљање

Ово тело је 1992. године објавило студију под називом „Интегрисани оквир за интерну контролу“ (*Internal Control – An Integrated Framework*). Овај документ је од историјског значаја за развој интерне и екстерне ревизије, јер представља први пример системског и документованог приступа овој области. У 2004. години, „Интегрисани оквир за интерну контролу“ је значајно модификован и унапређен. У циљу његовог осавремењавања

учињен је напор да се покрију сви аспекти управљања и контроле у пословању, тако да он данас обухвата пет главних подручја:

- Управљачко-контролно окружење (*Control environment*)
- Процена ризика (*Risk assessment*)
- Управљачко-контролне мере и активности (*Control activities*)
- Информације и извештавање (*Information and Communication*)
- Праћење (*Monitoring*)

Иако се у делу који се односи на информације препознаје значај информација и информационих система у пословном окружењу и њему припадајућем систему интерних контрола, мора се констатовати да је овај документ првенствено од значаја за општу (интерну и екстерну) ревизију а знатно мање за специјализовану (технолошку) ревизију. Такође, треба приметити да је КОБИТ у целини усклађен са КОСО оквирима, те да се може схватити као његова надградња и ужа специјализација са усмерењем на област ИС/ИТ.

б) Оквир за управљање ризиком

Исто тело (COSO) је у 2001. години започело пројекат израде „Интегрисаног оквира за управљање ризиком” (*Enterprise Risk Management – An Integrated Framework*). Мотивација за овај пројекат је пристекла из низа финансијских скандала који су му непосредно претходили (*Enron, Tyco International, Adelphia, Peregrine Systems, WorldCom*, итд) и који су указали на то да је област ризика у пословању била недовољно добро регулисана, како законском тако и стручном регулативом.

Овај оквир обухвата осам главних подручја:

- Интерно окружење (*Internal environment*)
- Постављање циљева (*Objective setting*)
- Препознавање догађаја (*Event identification*)
- Процењивање ризика (*Risk assessment*)
- Реаговање на ризике (*Risk response*)
- Управљачко-контролне мере и активности (*Control activities*)
- Информације и извештавање (*Information and communication*)
- Праћење (*Monitoring*)

Овај документ је дао снажан подстицај за развој у области управљања, оцене и мерења свих врста пословних ризика. Иако директно и детаљно не разматра област информатичких ризика, његов значај је велики и у овој области, будући да он поставља најшире оквире, принципе и стандарде на основу којих је могућа даља специјализација.

2.9.4. Стандарди Међународне организације за стандардизацију (ISO)

Постоји велики број међународних стандарда који се директно или индиректно односе на информационе и комуникационе технологије, њихову примену у пословним системима, па тако и на област ризика, контроле, управљања и ревизије у примени технологија.

Преглед свих ових стандарда превазилази обим овог рада. У Прилогу 4.2. дата је референтна листа са ознакама и називима најважнијих стандарда. На овом месту ћемо се задржати само на стандардима који непосредно регулишу област система за управљање информатичком безбедношћу. Ово пре свега због тога што је информатичка безбедност повезана са пословним ризицима највишег степена, тако да је та област природно у самом центру пажње сваке (на процени ризика засноване) технолошке ревизије. То је фамилија стандарда ISO 27000, чији су најзначајнији чланови, за сада, два стандарда: ISO 27001 и ISO 27002.

а) **Стандард 27001**

Пуни назив овог стандарда је *ISO/IEC 27001:2005 - Information technology – Security techniques – Information security management systems – Requirements*, али се најчешће користи његов скраћени назив *ISO 27001*. Овај стандард је донесен 2005. године, са циљем да дефинише оквире за успостављање система за управљање информатичком безбедношћу (*ISMS – Information Systems Management Systems*).

Будући да по својој суштини представља један скуп захтева, његова примена има мандаторну природу. То такође значи да је могуће упоређивање реалних система у погледу усклађености са овим стандардом. Уколико се овакав поступак спроведе од стране акредитованих сертификационих ревизора, у случају издавања позитивне оцене о усклађености, предметна организација може да добије званични сертификат о усклађености са овим стандардом.

ISO/IEC 27001 поставља пред руководство следеће захтеве:

- Да систематично испитује све ризике из области информатичке безбедности у организацији, водећи рачуна о претњама, слабостима и могућим последицама,
- Да испланира и успостави доследан и свеобухватан скуп управљачко – контролних и других неопходних мера за одговарајући третман (избегавање или пренос) неприхватљивих ризика,
- Да успостави одговарајуће управљачке процесе са циљем да се обезбеди континуирано функционисање свих управљачко – контролних мера против ризика.

Поступак сертификације о усклађености са *ISO 27001* по правилу се састоји од сертификационе ревизије која тече у три фазе:

- **Прва фаза** је прелиминарни и неформални преглед система за управљање информатичком безбедношћу, при којем се врши провера да ли постоји и у каквом стању се налази основна документација у организацији, као што су, на пример, Политика о информатичкој безбедности (*Information Security Policy*), Изјава о применљивости (*Statement of Applicability – SoA*) и План за управљање ризиком (*Risk Treatment Plan – RTP*). Поред тога, у овој фази долази до међусобног упознавања између ревизора и организације, што увелико олакшава одвијање следеће две фазе.
- **Друга фаза** представља детаљан и формализован процес ревизије усклађености, у току којег се врши појединачно и независно испитивање система („тачку по тачку”) у односу на сваки од захтева које Стандард поставља. Ревизори треба да се увере да је систем добро пројектован и изведен, као и да он заиста функционише и

да је делотворан. Овлашћење за спровођење оваквих ревизија имају тзв водећи сертификациони ревизори (*ISO/IEC 27001 Lead Auditors*). Успешно окончање ове фазе значи да је организација стекла сертификат о усклађености са стандардом *ISO/IEC 27001*.

- **Трећа фаза** подразумева периодичне прегледе током којих се стиче уверење да се систем за управљање информатичком безбедношћу у предметној организацији успешно одржава у стању усклађености са стандардом. Ови прегледи се обављају најмање једном годишње, али се могу обављати и чешће, посебно у случајевима када се ради о новоуведеним системима.

б) **Стандард 27002**

Овај стандард је најпре објављен 2005. године под називом *ISO/IEC 17799:2005*, да би касније, 2007. године био једноставно пренумерисан и поново издат, овога пута под називом *ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management*. Данашња верзија је заправо прерада верзије из 2000. године, која опет није била ништа друго до дословна копија изворног документа – британског стандарда BS7799:1999.

ISO/IEC 27002 даје препоруке за најбољу праксу у области пројектовања, увођења и редовног одржавања система за управљање информатичком безбедношћу.

Овај стандард се састоји од следећих 12 секција:

- Процењивање ризика (*Risk assessment*)
- Политика информатичке безбедности (*Security policy*)
- Организациони аспекти информатичке безбедности (*Organization of information security - governance of information security*)
- Класификација информација и управљање информатичким средствима и имовином (*Asset management - inventory and classification of information assets*)
- Персонални аспекти информатичке безбедности (*Human resources security*) – безбедносни аспекти запошљавања, премештања и одласка запослених
- Физичка безбедност и безбедост радног окружења (*Physical and environmental security*)
- Управљање разменом информација и оперативним процедурама (*Communications and operations management – management of technical security controls in systems and networks*)
- Контрола приступа (*Access control*) - ограничавање права приступа мрежама, системима, апликацијама, функцијама и подацима
- Набавка, развој и одржавање информационих система (*Information systems acquisition, development and maintenance*)
- Управљање инцидентима у информатичкој безбедности (*Information security incident management*) – приправност и одговарајуће реаговање на случајеве повреда информатичке сигурности
- Управљање непрекидношћу пословања (*Business continuity management*) – заштита, одржавање и опоравак најважнијих пословних процеса и система
- Регулативна усклађеност (*Compliance*) – обезбеђивање поштовања политика

информатичке безбедности, стандарда, закона и друге регулативе

За сваку од наведених дванаест области, овај стандард даје одговарајуће контроле информатичке безбедности, заједно са њиховим циљевима и пратећим упутствима за њихово увођење. За разлику од захтева датих у стандарду 27001, ове контроле нису (не могу да буду) обавезујуће за примену, пре свега због тога што се подразумева да ће свака поједина организација на основу овог стандарда приступити развоју сопственог система информатичких контрола који је примерен њеним конкретним потребама и специфичностима. Од стандарда опште применљивости, као што је овај, не може се очекивати да покрије све могуће специфичне потребе појединих организација.

2.9.5. Стандарди НИСТ

Од доношења „Савезног закона о управљању информатичком безбедношћу” (*FISMA – Federal Information Security Management Act*) 2002. године у САД је ступила на снагу обавеза да се све државне агенције морају придржавати Савезних стандарда за обраду информација (*FIPS – Federal Information Processing Standards*). НИСТ – „Национални институт за стандарде и технологију” (*NIST – National Institute of Standards and Technology*) је на савезном нивоу у САД задужен за стандарде и мерења у области технологија. Посебно одељење унутар Института, под називом *CSRC (Computer Security Resource Centre)* израдило је врло велики број публикација, препорука и стандарда, од којих је најзначајнији документ под ознаком *Special Publication 800-12; An Introduction to Computer Security: The NIST Handbook*.

Захваљујући својој универзалној применљивости, овај документ је познат и примењиван далеко изван граница САД и постао глобално прихваћена референца. Он покрива материју веома сличну оној у стандардима *BS 7799 (ISO17799/ISO27000)*, с тим да „Приручник” већину области обрађује далеко детаљније.

Поред приручника *SP-800-12*, треба поменути и стандард под називом *FIPS 200: Minimum Security Requirements for Federal Information and Information Systems*, који покрива 17 области и има обавезујућу снагу за све савезне агенције у САД.

У Прилогу 6.2 дат је списак свих FIPS стандарда и специјалних публикација института НИСТ.

2.9.6. Стандарди БСИ

Немачки савезни завод за информатичку безбедност (*BSI – Bundesamt für Sicherheit in der Informationstechnik*, енгл. *Federal Office for Information Security*) је владина организација задужена за регулативу и стандардизацију у области информатичке безбедности. Ова организација је издала збирку докумената под заједничким називом *IT Baseline Protection Catalogs (IT-Grundschutz Catalogs)*. Још увек се често користи и стари назив, који је званично престао да важи 2005. године: *IT Baseline Protection Manual (IT-Grundschutzhandbuch)*. „Каталози основне заштите информационих технологија”, како би гласио слободан превод назива, су, слободно се може рећи капитално дело у области заштите ИТ. Садржај импресивног обима (близу 3000 страна) је подељен у четири самосталне целине:

- **Опште информације.** Овај део даје увод и објашњава методологију и

одговарајуће моделе заштите ИТ коришћене кроз читав документ, као и улоге главних носилаца одговорности за заштиту ИТ

- **Каталози модула** (*Modules*). Овај део садржи пет каталога који покривају основне аспекте безбедности ИТ, подељене по тзв слојевитом моделу:
 - В 1: Генерички аспекти ИТ (*Generic aspects of IT*)
 - В 2: Безбедност инфраструктуре (*Security of the infrastructure*)
 - В 3: Безбедност ИТ система (*Security of the IT systems*)
 - В 4: Безбедност у мрежи (*Security in the network*)
 - В 5: Апликативна безбедност (*Security of applications*)
- **Каталози претњи** (*Threat catalogues*). Овај део даје детаљни преглед претњи и претећих сценарија који се могу јавити у појединим модулима. Претње су груписане у пет каталога:
 - Т 1: Виша сила (*Force majeure*)
 - Т 2: Организациони пропусти и недостаци (*Organisational shortcomings*)
 - Т 3: Људска грешка (*Human failure*)
 - Т 4: Техничка грешка (*Technical failure*)
 - Т 5: Намерни поступци, злоупотребе (*Deliberate acts*)
- **Каталози заштитних мера** (*Safeguard Catalogues*). Овај део садржи шест каталога у којима су детаљно изложене заштитне мере против претећих сценарија који се могу јавити у појединим модулима.
 - С 1: Инфраструктура (*Infrastructure*)
 - С 2: Организација (*Organisation*)
 - С 3: Персонал (*Personnel*)
 - С 4: Хардвер и софтвер (*Hardware and software*)
 - С 5: Комуникације (*Communication*)
 - С 6: Планирање за непредвиђене ситуације (*Contingency planning*)

Поред „Каталога”, БСИ је објавио још и три стандарда, који се посебно односе на поједине аспекте безбедности информатичких технологија (конкретно на системе за управљање информатичком безбедношћу, методологију за основну заштиту и на анализу ризика):

- BSI-Standard 100-1: Information Security Management Systems
- BSI-Standard 100-2: IT-Grundschutz Methodology
- BSI-Standard 100-3: Risk Analysis Based on IT-Grundschutz

2.9.7. Стандарди ИСФ

Форум за информатичку безбедност (*ISF – Information Security Forum*) је удружење организација и компанија чији је циљ стално унапређивање стања информатичке безбедности својих чланова. За двадестак година свога постојања (основан 1989.), Форум је израстао у водећи независни ауторитет у области информатичке безбедности у читавом свету. Форум данас има око 300 чланова, углавном најуспешнијих компанија у најразличитијим пословним областима (банкарство, телекомуникације, индустрија итд).

Форум издаје велики број публикација – стандарда, препорука, алата, извештаја студија и анализа итд. Нажалост приступ овим публикацијама је, осим у неколико изузетака, строгом политиком заштите интелектуалне својине ограничен искључиво на чланове Форума.

Један од изузетака је тзв „Стандард добре праксе” (*ISF Standard of Good Practice*) који је јавно доступан. Овај стандард је организован у шест главних делова који покривају следеће аспекте информатичке сигурности:

- Управљање безбедношћу (*Security Management*)
- Критичне пословне апликације (*Critical Business Applications*)
- Рачунарске инсталације (*Computer Installations*)
- Мреже (*Networks*)
- Развој система (*Systems Development*)
- Корисничко окружење (*End User Environment*)

Поред „Стандарда добре праксе”, Форум је реализовао низ пројеката од интереса за своје чланство, којима је покривена проблематика коју је чланство изабрало као најзначајнију и од заједничког интереса. У Прилогу 6.2. набројани су неки од ових пројеката

3. СТУДИЈА СЛУЧАЈА – ПРИМЕР РЕВИЗИЈЕ ИНФОРМАЦИОНОГ ПОДСИСТЕМА

3.1. УВОД

У радовима овакве врсте, студија случаја обично подразумева излагање неког конкретног, аутентичног примера из праксе са циљем да се илуструје неки општи, теоријски концепт. Међутим, у области интерне ревизије постоје извесна ограничења која не дозвољавају да се студија случаја спроведе на потпуно аутентичном примеру.

Као прво, интерни ревизор је етичким кодексом обавезан на поштовање принципа поверљивости, који га ограничава у изношењу информација до којих је дошао у поступку ревизије. Такође, када се нађе у улози консултанта – екстерног технолошког ревизора, дужан је да поштује одредбе споразума о поверљивости (*NDA – Non-disclosure Agreement*), који по правилу забрањују изношење у јавност података и сазнања до којих се дошло током учешћа у конкретном пројекту.

Да би се истовремено задовољила оба међусобно супростављена услова – аутентичност и тајност – задржана је аутентичност сценарија из неколико конкретних пројеката и сачињен агрегат њихових најилустративнијих елемената. При томе, уклоњене су или измењене све референце на конкретне актере – називи организација, организационих целина и физичких лица, тополошке и друге карактеристике система итд, како би се учинила немогућом свака корелација са стварним физичким и правним лицима и догађајима. При свему томе, учињен је максимум да се очува реалистичност изложене материје.

3.2. ОПИС СИТУАЦИЈЕ

Преметни систем је специјализовани апликативни систем наменски опредељен за подршку и управљање процесом електронског платног промета. Систем је развијен специјално за корисника у чијем се власништву налази и класификован је као пословна апликација од критичне важности за остварење укупних пословних циљева организације. Основна намена система је да обезбеди креирање, верификацију и прослеђивање налога за плаћање према пословним банкама, као и да омогући аутоматско преузимање извода односно привремених извода и њихово раскњижавање.

Главне карактеристике предметног система су следеће:

- Систем је реализован у трослојној архитектури. Веб браузер је у улози танког клијента (први слој) преко којег се приступа апликативном серверу. Пословна логика је имплементирана у форми веб апликације која се налази на том апликативном серверу (други слој), док се пословни подаци налазе на серверу наменске базе података (тећи слој).
- Сервер наменске базе података се налази у сталној вези са другим серверима пословног информационог система, односно према другим пословно-апликативним подсистемима, као што су: рачуноводство, плате (обрачун зарада), фактуре, кредитне обавезе, службена путовања, уговори, судске тужбе у случају

ненаплаћених потраживања итд. Наменска база података дизајнирана је тако да садржи само подскуп пословних података који је релевантан за конкретну пословну логику апликације, тј за електронски платни промет. Да би се одржао укупни интегритет (ажурност), ова база се налази у сталном процесу обостраног преузимања података са низом других база података у пословно-информационом систему.

- Веза према пословним банкама је реализована кроз изнајмљену (приватну) телекомуникациону линију од тачке до тачке (*Frame Relay – nailed-up connection*) на којој су дозвољене само једнострано инициране конекције, и то од корисника према банкама. Интернет не само да се не користи, већ је потпуно спречен сваки мрежни саобраћај између сервера овог подсистема и Интернета.
- Саобраћај се пакетски филтрира у оба смера, по строго рестриктивној листи дозвољених портова и ИП адреса. Све долазне мрежне конекције су спречене мрежном баријером (мрежна запрека, заклон – *firewall*). Сви сервери су адресирани тзв приватним ИП адресама. Јавне адресе се директно не користе, већ се конвертују на периметру приватне мреже (*NAT/PAT*).
- Конекције се штите елементима инфраструктуре јавних кључева – двоструким дигиталним потписом на сваком налогу за плаћање. Први пут, потпис се ставља на налог на рачунару крајњег клијента (смарт-картица и одговарајући читач) а други пут се налог потписује непосредно пред слање, коришћењем шифарског кључа садржаног у дигиталном сертификату који је банка издала кориснику
- Аутентификација на страни корисника је виšekратна – сви запослени који су овлашћени за рад на овом систему имају, поред корисничког имена и лозинке за приступ рачунару са којег приступају апликацији, још и смарт картицу заштићену личним идентификационим кодом (ПИН) за приступ припреми и слању налога за плаћање, односно његово дигитално потписивање.
- Ауторизација се спроводи у две равни – „по ширини и по дубини”. Наиме, права приступа аутентификованог корисника се проверавају посебно за приступ појединим сегментима апликације а посебно за приступ појединим табелама у бази података, односно подацима који се тамо налазе.
- У погледу физичке заштите, систем је покривен низом мера које предвиђају интерне процедуре о физичко-техничкој заштити информатичке опреме, као и општим и посебним мерама за заштиту од прекида пословања. Резервне копије података (резервни преписи – *backup*) раде се редовно, и то сваког дана инкрементално и сваке недеље кумулативно.

У току експлоатације, овај систем је у више наврата био предмет ревизије. Како су плаћања значајан део финансијских активности, овај апликативни подсистем је био у више наврата укључиван и у прегледе финансијске ревизије, од стране различитих екстерних ревизорских кућа. Такође, систем је био предмет анализе интерних ревизора према различитим методолошким приступима – на традиционални, финансијски оријентисан начин и на нешто савременији начин, какав се препоручује ревизорима информационих система. Такође, систем су прегледали и стручњаци за информатичку безбедност са циљем да утврде сагласност са важећим међународним стандардима у овој области. На крају, систем је подвргнут интегрисаној технолошкој ревизији. У овој студији случаја, приказаћемо конкретна искуства са сваким од наведених ревизорских приступа.

3.3. ПРИМЕРИ ТРАДИЦИОНАЛНОГ РЕВИЗОРСКОГ ПРИСТУПА

3.3.1. *Интерна ревизија – конвенционални приступ*

У овом примеру, интерна ревизија је добила задатак да прегледа процес платног промета. Опсег ревизорског задатка је морао да обухвати целокупни ток пословног процеса у области платног промета – плаћања обавеза и наплате потраживања. Циљеви ревизорског задатка су били да се провери постојање и примена процедура, примена и поштовање рачуноводствених политика и стандарда, као и да се испита и оцени систем интерних контрола унутар предвиђеног делокруга ревизорског задатка.

Предметни пословни процес и одговарајући систем контролних мера у овом примеру су веома сложени и од критичног значаја за укупно пословање. Пословно – апликативни систем који прати ове процесе обухвата следеће сегменте:

- плаћања према повериоцима по основу уговора,
- исплату зарада,
- плаћање кредитних обавеза,
- плаћања према јавним службама (таксе, ПДВ итд) као и
- прилив од продаје и наплате услуга и робе, накнаде штета итд.

Сложеност овог пословног процеса праћена је одговарајућим обимом и структуром контролних мера, које су успостављене тако да омогуће руководству да делотворно спроводи своје улоге и одговорности у управљању и контроли. Ток ревизије у овом примеру илустроваћемо само детаљним праћењем првог од пет наведених пословних сегмената – плаћање према повериоцима по основу уговора. Због непотребног обима и дуплирања (мултиплицирања) информација, остала четири сегмента овде изостављамо уз напомену да су ти подпроцеси по свом обиму и сложености слични првом сегменту, те да је укупан ток ревизије био приближно пет пута обимнији од онога што следи у даљем излагању.

Процес плаћања према повериоцима по основу уговора има две улазне тачке:

- евидентирање уговора – регистровање уговора, регистровање уговорног партнера под одговарајућом шифром добављача, евидентирање ПИБ-а и броја текућег рачуна добављача, и
- евидентирање промена по уговору – пристизање фактура за авансно плаћање или плаћање по извршеној услузи.

Излазна тачка је плаћање према повериоцу преносом средстава са сопственог рачуна на одговарајући рачун пословне банке повериоца.

Пословни процес пролази кроз контролне тачке К1 до К14, што је документовано одговарајућом контролном процедуром, имплементирано у пословно – апликативном систему и детаљно пропраћено ревизорском анализом и оценом.

К1. Уговори и пристигле фактуре најпре долазе у писарницу, где добијају деловодне бројеве и бивају заведени у документациони систем. Ова контролна тачка спречава губљење документације и омогућава њено даље праћење у

документационом систему.

K2. Уговори се уносе у пословно – апликативни систем, при чему се евидентирају основни подаци о добављачима, као што су назив добављача, порески идентификациони број (ПИБ) и број банковног рачуна. Сваки новоунесени добављач добија јединствени број из шифарника, за који се у бази података везује одговарајући запис са карактеристичним подацима добављача. Сваки претходно евидентирани добављач се идентификује преко јединствене шифре и броја ПИБ, што онемогућава дуплирање записа о истом добављачу.

Фактуре из писарнице прелазе у рачуноводство, где се наставља њихова обрада, уз пролазак кроз одговарајуће контролне тачке.

K3. Да ли пристигла фактура долази од партнера који је већ регистрован у регистру добављача? Само ако се при уносу броја ПИБ потврди идентитет добављача и његов број банковног рачуна, биће одобрена даља обрада.

K4. Да ли постоји уговор по основу којег је испостављена предметна фактура? Само ако се при уносу података о добављачу потврди идентитет одговарајућег уговора који је основа за фактурисање, биће одобрена даља обрада.

Следећа фаза обраде је захтев за добијање одобрења службе за праћење реализације уговора.

K5. Служба за праћење реализације уговора контролише да ли је испуњена одговарајућа уговорна обавеза. Ова контрола се врши на основу увида у фазу реализације уговора (потврде о примопредаји робе/опreme/уређаја/услуга) везано за конкретан уговор и одговарајућу фактуру.

K6. Уколико је претходна контрола била успешна, издаје се одговарајућа потврда да је испуњен услов за књижење обавезе и издаје предлог за плаћање. Ова контрола представља предуслов за улаз у следећу фазу процеса.

Даље, процес обраде се враћа у рачуноводство где се наставља даља обрада

K7. На основу претходних провера и добијеног одобрења за књижење обавезе и предлога за плаћање, рачуноводство евидентира обавезу и упућује документацију на даљу обраду у службу буџетске контроле.

Обрада се наставља у служби за праћење, реализацију и контролу буџета, на основу документације добијене од рачуноводства.

K8. Овде се обавља увид у одговарајућу буџетску ставку и врши контрола у односу на планирана средства буџета. Добијени предлог за плаћање, пропраћен доспелом фактуром мора да буде покривен расположивим буџетом у одговарајућој буџетској ставци. Тек ако је ова контрола успешна, биће настављена даља обрада.

Следећа фаза процеса одвија се у служби за финансије (трезор), којој се упућује извештај о доспелој обавези.

K9. Трезор (служба за финансије) свакодневно прими већи број доспелих обавеза. Оне се обједињују и контролишу у односу на актуелно стање средстава на текућем рачуну. Према утврђеним приоритетима, трезор је у обавези да састави листу за дневно плаћање, која ће бити реализована у току текућег радног дана. Ова контрола има за циљ да управља протоком готовине на текућем рачуну (*Cash Flow*). Плаћања се распоређују по данима у складу са планираним доспећем обавеза и потраживања, тако да се не угрози ликвидност организације. У противном, активирају се реактивни механизми у виду захтева за краткорочне позајмице и слично.

K10. Полазећи од дневне листе плаћања, формирају се појединачни налози за плаћање. Ови налози се контролишу у односу на укупну листу и уносе у одговарајући део пословно – апликативног система.

K11. Верификација формираних налога за плаћање обавља се од стране овлашћених лица, што представља финалну контролу пред само плаћање.

K12. Оператер који непосредно извршава плаћање има контролу против двоструког плаћања истог налога. Плаћање се врши електронским путем, тако што се пословној банци проследи налог за пренос средстава на банковни рачун пословног партнера у фактурисаном износу.

K13. Пословно – апликативни систем за платни промет има могућност за праћење стања на рачунима код пословних банака, путем добијања тзв привремених извода. Ови изводи представљају додатну контролу којом се потврђује да је предметна трансакција успешно обављена.

K14. Коначна контролна тачка у овом процесу јесте тзв раскњижавање. То је поступак у којем се врши сравњивање промена стања на рачуну са интерном евиденцијом о извршеним плаћањима.

Интерни ревизори су током ревизорског задатка пропратили свих четрнаест контролних тачака и констатовали да су одговарајуће процедуре на месту, да су у складу са законима, прописима, политикама и стандардима које уређују ову област, као и да се у потпуности поштују од стране овлашћених и задужених лица.

Напомињемо да је исти овакав поступак спроведен и за остала четири апликативна сегмента (исплата зарада, плаћање кредитних обавеза, плаћања према јавним службама и прилив од продаје и наплате). Ревизорски налази и мишљење су за ове сегменте такође били у потпуности афирмативни што је истакнуто и кроз одговарајуће оцене у извештају ревизије.

Важно је напоменути да су у току овог ревизорског задатка у потпуности поштовани стандарди о професионалној пракси интерне ревизије.

Конвенционални приступ огледао се у томе што су све интерне контроле анализирани и оцењиване пре свега са аспекта мере у којој оне подржавају одговарајуће управљачке процесе и служе као контролни инструменти надлежном руководству у испуњењу

његових улога и одговорности. Чињеница да су ове контроле имплементиране у форми једног информационог (под)система узета је у обзир само утолико што је препозната потреба да се ревизија не може обавити без техничке помоћи информатичких стручњака. Њихова улога се, међутим, сводила на неопходну подршку у приступу, руковању и давању неопходних објашњења и тумачења рада предметног информационог система, коју су информатички стручњаци пружали ревизорима на њихов захтев. На пример, кад год би ревизори имали потребу да се увере у тачност, целовитост и валидност података, од информатичке подршке се захтевало да обаве одговарајуће оперативне радње на систему – генерисање упита, разврставање и сортирање података, табеларна израчунавања, састављање одговарајућих извештаја и слично. Такође, ови стручњаци су били задужени за давање уверења ревизорима у погледу поузданости рада и других перформанси система, као и за проверу исправности поступака лица која у току пословних процеса непосредно рукују предметним системом.

3.3.2. *Интерна ревизија – технолошки приступ*

У овом примеру, ревизорски задатак је поновљен са истим делокругом и са врло сличним циљевима. Конкретно, поред циљева који су постављени у претходном задатку, додат је још један: оценити адекватност примењених софтверских решења као подршке пословном процесу електронског платног промета, као и потенцијалне ризике и могуће слабости.

За потребе овог задатка, састављен је тим од специјалиста за финансијску ревизију и специјалиста за ревизију информационих система.

Финансијски ревизори су у потпуности поновили поступке који су наведени у претходном примеру. Припадајућом процедуром за овај пословни процес одговарајуће контролне тачке су статички дефинисане, тако да понављањем ревизорског задатка добијамо практично исти резултат све дотле док се не промени пословна логика, неки од модула пословно – апликативног система или док не дође до значајнијих одступања у погледу поштовања процедуре од стране оперативног особља.

Суштинска новост коју у овом примеру имамо у односу на претходни јесте у присуству ревизора за информационе системе и у њиховом приступу овом ревизорском задатку. Ревизори информационог система су извршили низ провера у области тзв генералних и апликативних контрола информационог система. Опште (генералне) контроле су уграђене у опште информатичке процесе и сервисе (на пример развој, набавка и имплементација система, администрација система, управљање променама, управљање софтверским корекцијама (*patch management*), безбедност, организациона структура ИС/ИТ), док се апликативне контроле везују за имплементацију пословне логике у информационим системима (на пример тачност, целовитост и валидност података, потврђивање трансакција, аутентификација, ауторизација, раздвајање дужности итд).

У општем случају, обим и сложеност контрола које се срећу у реалним информационим системима средњег или високог нивоа сложености је такав да се не може очекивати да све оне буду обухваћене једним ревизорским задатком. Полазећи од циљева конкретног задатка и руковођени приоритетима у односу на конкретни пословно – апликативни подсистем, као и на искуству заснованој неформалној процени ризика, ревизори су се усмерили на оцену конкретног подскупа општих и апликативних контрола.

Опште (генералне) контролно – управљачке мере:

- ОК1. администрација система – корисници и корисничке групе
- ОК2. управљање променама
- ОК3. управљање корекцијама
- ОК4.1. безбедност – антивирусна заштита
- ОК4.2. безбедност – филтрирање саобраћаја и мрежне баријере (запреке, заклони)
- ОК4.3. безбедност – противинтрузиона средства – системи за откривање и спречавање упада (*IDS/IPS – Intrusion Detection/Prevention Systems*)
- ОК4.4. безбедност – заштита тајности, шифровање, инфраструктура јавних кључева (*PKI*)
- ОК4.5. расположивост и непрекидност рада – управљање резервним копијама (преписима) и опоравак система (*Backup/Restore*), непрекидно напајање
- ОК5. контрола приступа

Апликативне контролно – управљачке мере:

- АК1. тачност, целовитост и валидност уноса података
- АК2. тачност, целовитост и валидност излазних података
- АК3. аутентификација корисника
- АК4. ауторизација корисника, додела корисничких улога, принцип минималних овлашћења, принцип неопходне информисаности
- АК5. потврда трансакција
- АК6. раздвајање (сепарација, сегрегација) дужности
- АК7. усклађеност контролних збирова
- АК8. вођење дневника трансакција (*logging, audit trails*)
- АК9. корисничко искуство, прихватљивост и продуктивност: једноставност употребе, помоћ кориснику, превенција корисничких грешака

Ревизори су установили да је стање општих и апликативних контрола у подсистему за електронски платни промет задовољавајуће. Нису пронађени никакви пропусти у систему – констатовано је да све набројане контроле постоје и да су функционалне. Извештај је у целини био афирмативан и без значајнијих примедби.

3.3.3. Екстерна ревизија

Задатак екстерне ревизије је пре свега да пружи објективно и независно стечено мишљење о исправности финансијских извештаја једне организације. Ово се углавном односи на релевантност, тачност и целовитост предметних финансијских извештаја. Иако се делокруг и обим рада екстерних ревизора и циљеви екстерне ревизије овако уско постављају не само у теоријском разматрањима, већ и у конкретној пракси, па тако и у клаузулама склопљеног уговора о услугама екстерне ревизије, уочљив је напор екстерних ревизора да се у обављању својих задатака прошире и на друге аспекте пословања, не само финансијске, како би се стекао што бољи увид у рад предметне организације.

У том смислу, екстерна ревизија показује све веће интересовање за неке технолошке аспекте, пре свега за стање генералних и апликативних контрола, затим за

информатичку подршку, алате и технике које користи интерна ревизија, као и за општи ток процеса и уређеност интерне, па и технолошке ревизије у организацији.

У конкретном случају, екстерна ревизија је затражила на увид све извештаје интерне ревизије, међу којима је био и извештај о ревизији система електронског платног промета. Након анализе ових извештаја, обављен је разговор са руководиоцем интерне ревизије, у којем су расветљени неки детаљи о току и конкретним поступцима интерних ревизора. У погледу система за електронски платни промет, екстерна ревизија није предузела ништа изван оквира претходно извршених задатака интерних ревизора.

Коначни извештај екстерне ревизије се ни у једном свом делу није дотицао подсистема за електронски платни промет, нити је разматрао било какве технолошке аспекте пословања организације. У целини афирмативан, овај извештај се задржао у оквирима оцене финансијског извештавања. У њему није било никаквих назнака да се екстерна ревизија бавила било чиме изван области финансија, па тако ни контролама у области електронског платног промета.

3.4. ПРИМЕР АНАЛИЗЕ УСКЛАЂЕНОСТИ СА БЕЗБЕДНОСНИМ СТАНДАРДИМА

Независно од претходно изнесених примера интерне и екстерне ревизије, специјализовано одељење за информатичку безбедност у предметној организацији спровело је анализу усклађености са безбедносним стандардом *ISO/IEC 27001* којом је био обухваћен, поред осталог, и пословно – апликативни подсистем за управљање електронским платним прометом. Анализа је спроведена у оквиру пилот-пројекта, чији је циљ био да се процени спремност организације за стицање званичног сертификата *27001*. У оквиру пројекта, група специјалиста из састава организације развила је контролну листу за проверу усклађености и по тој листи спровела провизорну анализу, како би се откривене слабости отклониле пре ангажовања званичног сертификационог ревизора и на тај начин умањили трошкови процеса сертификације.

Иако ова анализа није била вођена од стране овлашћеног сертификационог ревизорског тима, њени резултати се могу сматрати поузданим, с обзиром на стручност и мотивацију тима који ју је спровео. Контролна листа је у потпуности обухватала структуру и садржај стандарда и предвиђала прибављање одговора на укупно 179 ревизорских питања, груписаних у 35 контролних група, којима је покривено следећих 10 области:

- Политика информатичке безбедности
- Организациони аспекти информатичке безбедности
- Класификација информација и управљање информатичким средствима
- Персонални аспекти информатичке безбедности
- Физичка безбедност и безбедност радног окружења
- Управљање разменом информација и оперативним процедурама
- Контрола приступа
- Развој и одржавање система
- Управљање непрекидношћу пословања
- Регулативна усклађеност

Укупан обим анализе далеко превазилази оквире овог рада. Овде је могуће само коментарисати најзначајније налазе и укупан резултат.

Иако су резултати пројекта указали на одређени број тачака у којима организација не испуњава захтеве стандарда, ниједна од примедби није се директно односила на предметни пословно – апликативни систем. Другим речима, за предметни систем (електронски платни промет) није установљено да је директно утицао на укупну меру неусклађености организације са стандардом *ISO/IEC 27001*.

3.5. ПРИМЕР ИНТЕГРИСАНОГ РЕВИЗОРСКОГ ПРИСТУПА

3.5.1. Делокруг и циљеви ревизорског задатка

У овом примеру, ревизорски задатак је дат тиму уско специјализованих технолошких ревизора. Делокруг задатка је поново ограничен на пословно – апликативни систем за управљање електронским платним прометом. Циљ задатка је био да се утврди да ли у систему за електронски платни промет постоје било какви ризици који потичу од примене информационих технологија а који могу да угрозе интересе организације у погледу безбедности, економичности, ефикасности или ефикасности процеса електронског платног промета или других, са њим повезаних, пословних процеса.

3.5.2. Анализа архитектуре

Архитектура система подразумева структуру, топологију, расподелу и повезаност функционалних целина, организацију хардвера, системског и апликативног софтвера, имплементацију пословне логике, поделу улога и одговорности корисника, интеракцију корисника са системом и све друге карактеристике које у потпуности одређују предметни систем. За анализу архитектуре неопходно је извршити увид у сву расположиву документацију о систему. Пре свега, потребно је прегледати пројектну документацију – техничке захтеве, идејни и главни пројекат. Такође, веома значајан је и пројекат изведеног стања, као и извештаји о актуелном стању система који се могу добити из система за управљање променама – системског инвентара и конфигурационе базе података.

На основу ових информација, ревизори стичу основно знање о систему – о његовој намени, о томе како је замишљен, како је реализован и како (би требало да) функционише.

Иако ова анализа може да укаже на пропусте учињене у фази пројектовања или имплементације, њен основни значај је у томе што пружа информативну основу за рад у следећим фазама. Она ревизорима даје увид у тзв „власничку перспективу” - поглед на систем из перспективе организације која тај систем користи и њиме руководи.

3.5.3. Енумерација мрежних уређаја, сервера и радних станица

У овој фази се открива присуство рачунара и мрежних уређаја унутар предметних мрежних сегмената. У општем случају, ово се своди на слање *ICMP* пакета типа 8 према

ИП адресама у оквиру одређеног сегмента. Пакети типа 8 у *ICMP* протоколу су тзв „ехо захтеви” - сваки уређај који добије такав захтев дужан је да одговори на њега тако што пошаље уназад одговарајући „ехо” или „одјек”. У случају грешке, одредишни рачунар или успутни рутер шаљу уназад одговарајуће одговоре: *network unreachable*, *host unreachable*, *TTL exceeded in transit* и слично, чиме се полазној страни ставља до знања да постоје разлози због којих није могуће добити одговор на захтев.

Брзо одашиљање оваквих захтева редом према свим адресама у сегменту (тзв *pingsweep*) и бележење одговора представља најлакши начин за енумерацију „живих” мрежних адреса. Проблеми настају ако је неким мрежним филтером спречен *ICMP* саобраћај на некој од адреса или на целом мрежном сегменту. Тада су ревизори принуђени да се прикључе локално на предметни адресни сегмент и да енумерацију обаве тзв *ARP* скенирањем: за све адресе из сегмента генерише се редом *ARP* упит „ко има адресу *x . x . x . x*” и забележе добијени одговори.

Алати којима се ревизори служе при овакој енумерацији су бројни. Најпознатији међу њима су: *ping*, *tracert*, *angryIP*, *ICMPquery*, *hping3*, *thc-rut*, *arping* и *nmap*.

Резултати ове фазе се у општем случају могу разликовати од документације коју поседује власник, што представља индикацију да су присутни недостаци у процесима управљања променама у систему и у инвентару информатичких средстава. Зато је веома важно да се поступак енумерације спроведе са што мање ослањања на власничку документацију, односно да се енумерацији приступи као да се ради о потпуно непознатом систему.

У конкретном случају, број откривених ИП адреса се поклапао са стањем у добијеној документацији, што је ревизија позитивно оценила.

3.5.4. Енумерација сервиса, „скенирање портова” (*port scanning*)

На свим откривеним адресама покренут је поступак енумерације мрежних сервиса. То је урађено скенирањем *TCP* и *UDP* портова на свим адресама у сегменту (сегментима). Овај поступак може бити обављен различитим алатима (*atar*, *nmap*, *superscan*, *thc-probe*). У овом примеру коришћен је *nmap*. Скенирање *TCP* портова обављено је у два пролаза: први пут је коришћен метод отворене (недовршене) конекције (*syn scan*) док је у другом пролазу коришћен метод пуне конекције (*tcp connect scan*). Резултати су показали да између мрежног сегмента у којем су били лоцирани ревизори и предметног мрежног сегмента не постоји функција филтрирања мрежног саобраћаја, што значи да је сервисима у предметном сегменту могуће приступити из удаљених сегмената локалне мреже.

Откривени сервиси („отворени” портови) јасно су указивали на разлике у намени појединих рачунара – радне станице и сервери. Сервери су издвојени у посебну групу, ради додатне анализе. Као и у претходној фази, установљена је подударност стварног стања са стањем у документацији.

3.5.5. Идентификовање оперативних система

Откривени рачунари и мрежни уређаји се подвргавају даљој анализи са циљем да се утврди врста оперативног система која је на њима у раду. Резултати се упоређују са документацијом и, у случају одступања, ручно проверавају. Циљ је да се открију одступања у односу на извештај о системском инвентару опреме, као и у односу на усвојене компанијске стандарде у организацији. Уколико се оваква одступања установе током ревизије, то указује на пропусте у процесима руковођења и захтева одговарајућу реакцију кроз ревизорски извештај, односно ревизорску оцену и препоручене корективне мере.

У овом примеру оперативни систем на серверима је био *MS Windows 2003* а на радним станицама *MS Windows XP Professional*, што је било у складу са документацијом добијеном из система за управљање променама.

Алат коришћен за идентификовање оперативних система био је *nmap*. За контролу резултата коришћен је *xprobe2*.

3.5.6. Идентификовање верзија и сервисног статуса

За све отворене портове подразумева се сервис који се уобичајено или према стандарду везује за те портове. Међутим, у пракси се често срећу одступања од општег случаја, која могу да буду последица намере али исто тако и последица погрешног конфигурисања. Зато је препоручљиво да се за сваки од сервиса утврди његов тачан идентитет а по потреби и његов сервисни статус – верзија, стање софтверских корекција, сервисни пакет и слично.

Најједноставнији али и најмање поуздан начин јесте регистровање одзива који се добија од сервера при конекцији на дати порт (*banner grabbing*). Већина сервиса у својој најосновнијој конфигурацији ради тако да се „представи” другој страни при првој конекцији. То је обично неки текст или комбинација текста и бинарног садржаја који идентификује произвођача, врсту и назив сервиса, његову верзију и слично. Међутим, за већину сервиса је могуће изменити садржај овог текста, што многи администратори система чине намерно како би онемогућили неовлашћеним лицима да дођу до информација којима се идентификују њихови сервиси. Уколико имамо основа да сумњамо у аутентичност серверског представљања, потребно је да искористимо неки од алата који су опремљени могућношћу да ову идентификацију обаве без ослањања на текст поруке којом се сам сервис представља. Ови алати располажу логиком која региструје суптилне разлике у реаговању различитих сервиса на побуде које им се упућују. Овај поступак се зове упоређивање отисака (*fingerprinting*) и у стању је да „на даљину” пружи доста поуздане одговоре о идентитету, верзији и сервисном статусу удаљених сервиса и припадајућих оперативних система. У конкретном случају, коришћен је *nmap*, док је за контролу појединих случајева коришћен и *atar*.

Уколико се установе значајнија одступања од стања у документацији, потребно је обавити „ручну” контролу директним приступом ревизора предметном рачунару.

У конкретном случају, утврђено је да су сервери и радне станице ажурни у погледу примењених сервисних пакета и софтверских корекција.

3.5.7. Идентификовање слабости (*vulnerability scanning*)

У следећој фази, технолошка ревизија обавља идентификовање конкретних слабости на мрежним уређајима, серверима и радним станицама.

Слабости (*vulnerabilities*) једним делом потичу од грешака у софтверу (системском или апликативном) за које се зна да могу бити злоупотребљене у циљу нарушавања интегритета, тајности или непрекидне расположивости информатичких ресурса. То су софтверске грешке настале током пројектовања и/или развоја софтвера (тзв „багови”, од енгл. *bug*, што значи буба). Произвођачи (власници технологија) својим корисницима редовно стављају на располагање софтверске корекције којима се ови недостаци отклањају. На корисницима лежи одговорност да успоставе редовне процедуре и контроле за благовремену примену ових корекција, што се спроводи кроз процесе редовног сервисирања софтвера. Уколико налази технолошке ревизије покажу да у систему постоје слабости ове врсте, то значи да су процеси контроле мањкави и да је организација изложена ризику од злоупотребе софтверских грешака у саставу информacionих технологија којима управља.

Другим делом, слабости потичу од пропуста у конфигурисању, редовном одржавању и администрацији система. Чак и систем у којем нема „багова” може се лошим руковањем довести у стање непоузданог, несигурног рада или у стање које може бити злоупотребљено на неконтролисан начин. Ако ревизија открије ову врсту слабости, то указује на пропусте у систему интерних контрола у некој од области управљања информacionим технологијама у организацији.

За откривање слабости користе се специјализовани алати (*vulnerability scanners*). У конкретном примеру коришћена су два алата – *ISS Internet Scanner* и *Nessus*.

Резултати ове фазе ревизије потврдили су да су у предметном систему сви сервери и радне станице ажурно сервисирани. Примењене су најновије верзије софтвера, сви расположиви сервисни пакети и одговарајуће софтверске корекције, тако да по том основу нема пропуста који би могли да буду злоупотребљени.

Један од сервиса на апликативном серверу по процени ревизора захтевао је посебну анализу. Скенирање портова показало је да је на апликативном серверу отворен порт 1433/*TCP*, за који се касније испоставило да потиче од система за управљање базама података, конкретно *MS-SQL*, који је инсталиран и покренут на овом серверу. Анализа архитектуре указивала је на то да се на апликативном серверу не налази никаква база података. Са друге стране, овај сервис је био уредно заведен у систем за праћење промена и као такав био присутан и у конфигурационој бази података, редовно сервисираан и стално активан. Нико од одговорних лица, међутим, није био у стању да објасни ко је власник овог сервиса, зашто је он покренут и чему служи.

У току анализе слабости, утврђено је да управо ова инстанца *SQL* сервера има тривијалну лозинку за системског администратора, коју је било веома лако открити погађањем, тако да ју је аутоматски открио један од скенера.

3.5.8. Налази и мишљење ревизије; препоручене мере

Извештај ревизије је у целини био афирмативан и садржао је само једну примедбу. Она се односила на откривени SQL сервис и на тривијалну администраторску лозинку која је на њему откривена. Процена ревизора је била да ова слабост уноси веома висок (критичан) степен ризика у укупан информациони систем. У том смислу, препоручено је да се утврди намена сервиса и власник одговарајућег пословног процеса. У случају да је постојање SQL сервиса неопходно за пословну логику апликације, лице одговорно за администрацију мора да у најкраћем року промени лозинку. У случају да је сервис непотребан, наложено је да се исти угаси и деинсталира.

3.6. ЕКСПЕРИМЕНТАЛНИ ТЕСТ НА ПРОБОЈ (КОНТРОЛИСАНИ НАПАД СА ЕСКАЛАЦИЈОМ)

3.6.1. Моштивација

Након ревизорског извештаја утврђено је да не постоји никаква веза откривеног сервиса са предметним системом за електронски платни промет нити са било којим другим пословним процесом у организацији. Шта више, у оквиру те MS-SQL инстанце није било никаквих креираних табела и база података, што је додатно указивало на то да је сервис сувишан. Није се могло са сигурношћу утврдити како и зашто је дошло до тога да се један такав сервис покрене на апликативном серверу, где је очигледно био потпуно непотребан. Вероватно је да се у врло раној фази развоја неко из развојног тима одлучио за то како би могао да тестира апликативну логику у оквиру једне хардверске платформе, „локално“, без потребе за ангажовањем посебног сервера за базу података. Касније, при пријему апликативног сервера у продукцију, овај сервис је унесен у конфигурациону базу, без контроле да ли је заиста потребан или не. Од тог тренутка на даље овај сервис је третиран као и сви други делови система – нико није тражио његово искључење и он је по инерцији одржаван у оперативном стању.

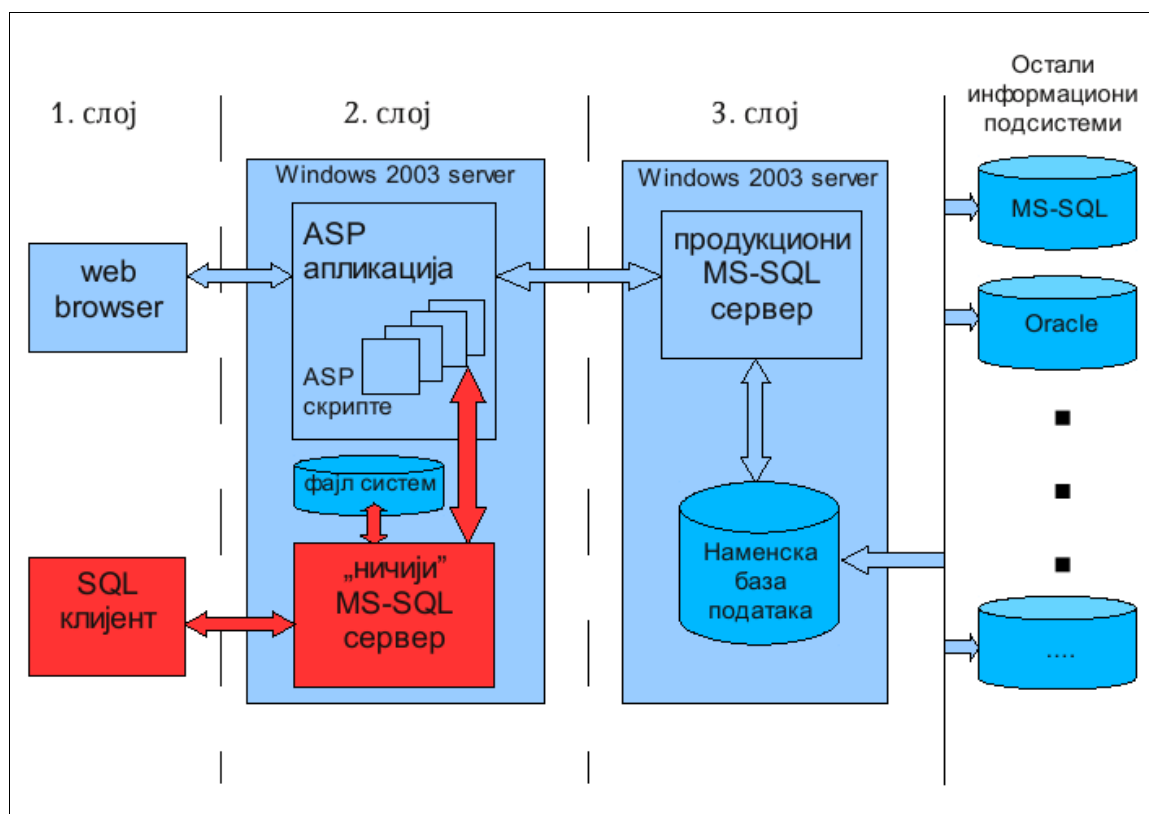
Постављено је, међутим, питање зашто су ревизори тако високо оценили ризик од присуства овог сервиса. Доведене су у сумњу ревизорске процене о томе какве и колике последице овај пропуст може да има на пословне процесе у организацији. Изнесено је мишљење да могућност злоупотребе базе података која је „празна“, не служи ничему и не садржи никакве податке не треба да се третира као нешто алармантно, те да су ревизорске процене претеране или чак штетне, јер без основа узнемиравају руководство и одвлаче им пажњу са других, значајнијих, питања.

Ревизори су предложили да се изведе експеримент у којем би се на контролисан начин извео напад на реални информациони систем и дошло до практичне демонстрације могућих последица таквог напада. Добијено је одобрење од највишег руководства, након чега се приступило реализацији пробојног (пенетрационог) теста. Задатак је био да се методама етичког хаковања демонстрирају све могуће последице и размера штете, с тим да се позната лозинка администратора користи као искључиви вектор напада.

3.6.2. Контролисани напад

а) Напад на апликативни сервер

Први корак напада је пријава у *MS-SQL* систем на апликативном серверу путем корисничког налога администратора и тривијалне лозинке. Конкретно, то је изведено коришћењем програма **sqlcmd.exe**, премда је могао да се употреби било који од великог броја расположивих *SQL* клијената. Будући да је нападач пријављен као системски администратор, *MS-SQL* му дозвољава извршавање команди локалног оперативног система, путем одговарајуће процедуре (*extended stored procedure: xp_cmdshell*). Ове команде ће бити извршене у сигурносном контексту *MS-SQL* процеса (*MSSQLSERVER service*), што је у овом случају контекст локалног администратора оперативног система, пошто је *MS-SQL* инсталиран без модификација (*default*), те је одговарајући процес као такав био учлањен у групу локалних администратора.



Слика 5: Напад на апликациони сервер

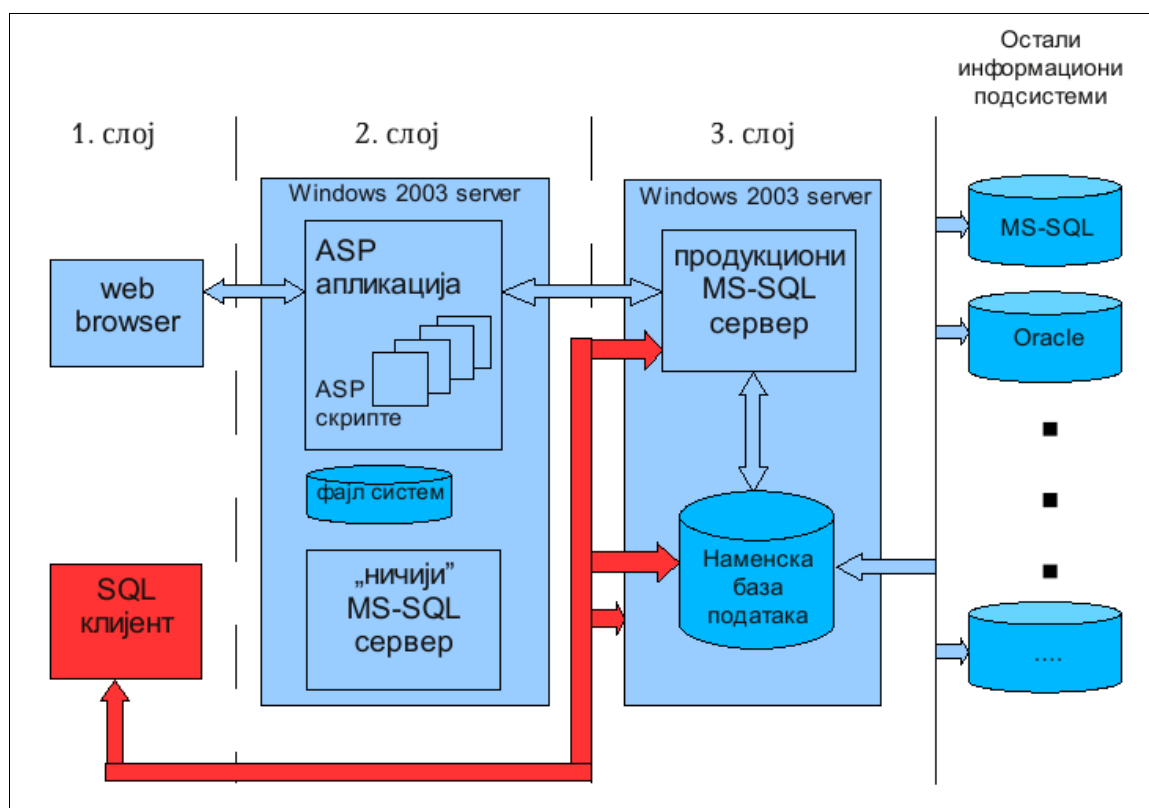
Према томе, коришћењем **sa** налога, нападач је добио права приступа локалном оперативном систему у рангу локалног администратора. У овом тренутку, једино средство за извршавање команди које му стоји на располагању јесте процедура **xp_cmdshell**, што га ограничава само на извођење конзолних команди и то оних које током свог извршења не захтевају интерактиван унос од стране корисника.

За праћење даљег тока напада је важно напоменути да нападач има пуну контролу над локалним системом датотека, што укључује и датотеке са *ASP* скриптама (*ASP – Active*

Server Pages). Овлашћења која поседује као **sa** корисник и средства којима располаже (**xp_cmdshell**) дају му могућност да их прегледа, копира, брише или мења њихов садржај.

б) Напад на сервер наменске базе података

Ова апликација је реализована тако да се за приступ бази података не користи тзв имперсонализација. То значи да се након аутентификације и ауторизације корисника, апликативна логика обрађа SQL серверу увек са истим, статички дефинисаним корисничким налогом а не са налогом корисника чија је сесија у току. Да би овакав приступ могао да се реализује, неизбежно је експлицитно навођење корисничког имена и лозинке у ASP скрипти која служи за успостављање конекције са базом података.



Слика 6: Напад на сервер продукционе базе података

Нападач је прегледом ASP скрипти, пронашао корисничко име и одговарајућу лозинку којима се апликација служи за приступ серверу наменске базе података (корисник: **epp**, лозинка: **epppassword**). Ово му је дало могућност да се конектује на сервер наменске базе података, на исти начин како је то претходно урађено са MS-SQL инстанцом на апликативном серверу.

Следећи корак је пријава на продукциони MS-SQL сервер коришћењем имена и лозинке пронађених у претходном поступку (**epp/epppassword**). Корисничка овлашћења сада нису на администраторском нивоу, али су довољно висока да се преко њих реализује приступ свим каталозима база података и одговарајућим табелама у оквиру датог сервера. У комбинацији са претходно прибављеном контролом на апликативном серверу,

то сада представља пуну и неограничену контролу над целом апликацијом за платни промет: токови извођења апликативне логике (ASP скрипте), опис структуре целе базе и свих типова података, као и сами подаци су у потпуној власти нападача.

Овде је важно напоменути да, поред осталог, нападач сада има и приступ неким системским табелама на MS-SQL серверу, међу којима је и системска табела **sysxlogins**, у којој се налазе подаци потребни за аутентификацију корисника – корисничка имена и „хешеви” одговарајућих лозинки („хеш” - енгл. *hash, digest* – једносмерно шифровани текст лозинке). Ово је веома значајно за даљи ток напада

в) Напад на корисничку лозинку системског администратора

Када је доступна системска табела **sysxlogins**, даљи поступак разбијања корисничких лозинки на MS-SQL серверу није претерано компликован. Он је детаљно приказан у доступној литератури. Према једном од извора (*David Litchfield: Microsoft SQL Server Passwords* [19]), издвојен је „хеш” лозинке системског администратора (**sa**) и нападнут помоћу речника. Програм за напад (*SQLCrack*) компајлиран је из незнатно модификованог изворног кода у језику C, приложеног уз [19]. За напад су коришћене посебно припремљене збирке личних имена и презимена као и речници енглеских и српских речи.

После релативно кратког времена, лозинка је успешно откривена (**astro41**). Тиме је напад на продукциони сервер завршен. По аналогiji са претходно изложеним нападом у тачки (а), нападач сада има права приступа у рангу локалног системског администратора на оперативном систему и системског администратора базе података (**sa**) на продукционом серверу, што је довољно за апсолутну контролу над овим сервером.

г) Напад на остале делове информационог система

Већ је речено да је подсистем за платни промет заправо само један од подсистема у саставу једног сложеног и знатно ширег информационог система, као и да се налази у сталној вези са извесним бројем других подсистема у окружењу. Анализом продукционе базе података, откривени су одговарајући механизми преко којих се наменска база података електронског платног промета синхронизује (реплицира) са базама у осталим деловима информационог система.

Иако су ови подаци познати ревизорима још из фазе анализе архитектуре система, поштован је договор да се током пробојног (пенетрационог) теста као вектор напада користи искључиво лозинка откривена током интерне ревизије (Види тачку 3.5.8 *Налази и мишљење ревизије; препоручене мере*).

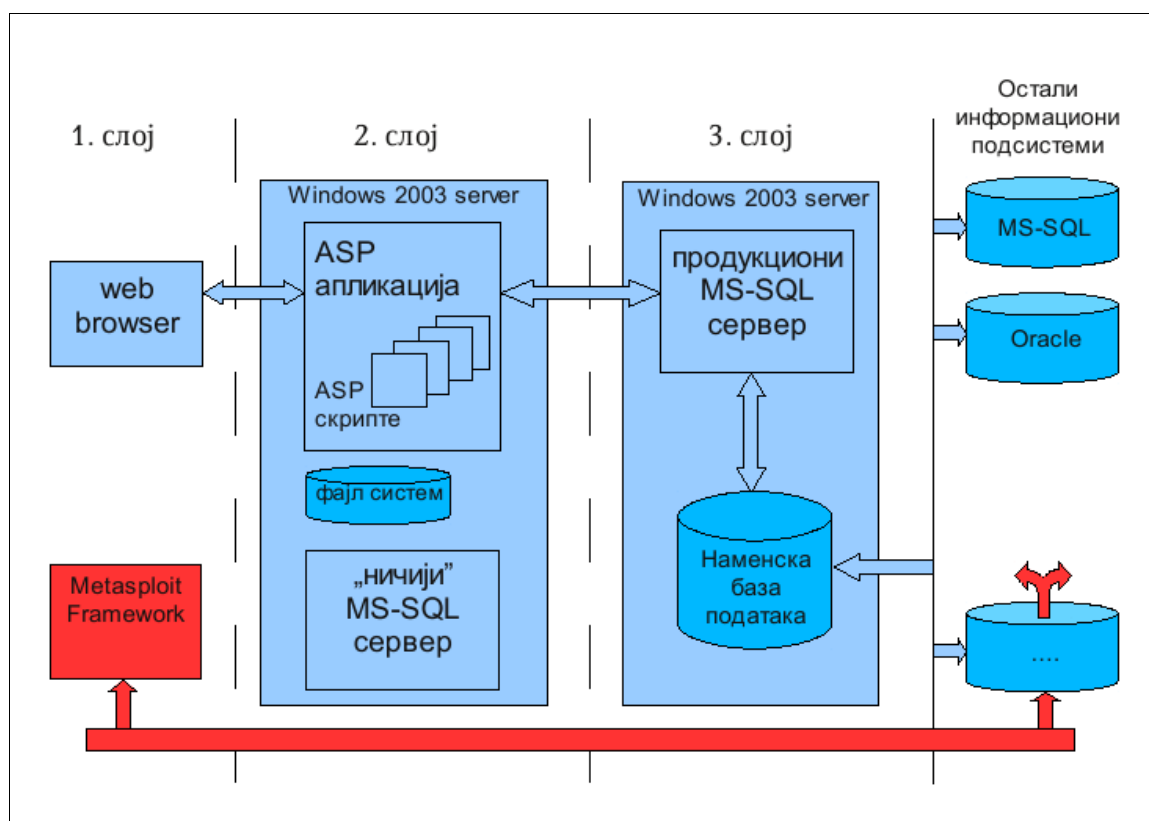
Анализом продукционе базе, извршена је енумерација свих сервера са којима је електронски платни промет у вези. Пошто ови сервери не припадају систему електронског платног промета и као такви нису били обухваћени конкретним ревизорским задатком, било је потребно да се према њима примени посебан поступак „напада на црну кутију” (*black box penetration test*), који је приказан даље у тачки 3.6.3.

3.6.3. Ескалација напaда

Утврђено је да наша апликација има везу са укупно 12 база података, које су смештене на укупно 5 различитих сервера (једна *Oracle*, на оперативном систему *HP-UX* и четири *MS-SQL* на оперативном систему *Windows Server 2003*).

Према свих пет сервера обављен је комплетан поступак идентификовања сервиса, оперативних система, њихових верзија, присуства софтверских корекција, сервисних пакета и идентификовања њихових слабости. Практично, за сваки од њих је поновљен цео поступак технолошке ревизије, са изузетком анализе архитектуре која овде није вршена (*black box penetration test*).

Испоставило се да су свих пет сервера у веома лошем сервисном стању. На њима је у просеку недостајало по десетак софтверских корекција/закрпа, од којих су неке биле рангиране као критичне по значају.



Слика 7: Ескалација напaда

Овом чињеницом даљи ток напада био је максимално поједностављен. На нападачевој радној станици покренут је *Metasploit Framework*. Уношењем одговарајућих кодова за недостајуће корекције, пронађени су одговарајући модули за експлоатацију конкретних пропуста (*exploits*). Њима су придружени додатни функционални модули (*shellcode*, *payload*) и преостали ток напада је био потпуно аутоматзован. За мање од 10 минута, свих пет сервера имало је на себи инсталиран **meterpreter**. Тиме је нападач остварио потпуну контролу над свим централним серверима пословног информационог система.

По завршетку овог контролисаног напада, накнадна анализа је показала како је дошло до тога да централни сервери буду у тако лошем сервисном стању. Испоставило се да су предметни сервери, заједно са пословним апликацијама и базама података испоручени од стране добављача који је на себе преузео уговорну обавезу одржавања целокупног система (хардвера и софтвера). Једна од одредби уговора изричито је забрањивала било какве измене на систему од стране купца, укључујући и инсталирање софтверских корекција и сервисних пакета. Нове верзије такође нису могле да буду инсталиране, због лиценцих обавеза које је испоручилац преузео у моменту интеграције система, а неке од њих су биле и некомпатибилне са појединим апликативним модулима, тако да би њиховом инсталацијом била угрожена и основна функционалност система.

3.7. ГЛАВНИ НАЛАЗИ СТУДИЈЕ СЛУЧАЈА

Изложени пример потврђује тезу да се једностраном применом традиционалних ревизорских метода и парцијалним технолошким приступом не може обезбедити пуна заштита организације од технолошки оријентисаних ризика, чак и уз доследну примену свих расположивих професионалних стандарда и препорука. Показано је да чак и најмањи организациони, техничко – технолошки или процедурални пропуст може да доведе до огромних последица по укупну безбедност организације. У конкретном случају систем је имао само једну слабу тачку, али се испоставило да је и она довољна да у случају циљаног напада доведе до компромитовања целокупног система за управљање информатичком безбедношћу.

Како је дошло до тога да ова слаба тачка остане неоткривена, упркос толиком броју ревизија? Ако по том питању детаљније анализирамо сваки од изложених ревизорских приступа долазимо до неколико запажања која можемо издвојити као кључне налазе у овој студији случаја.

Као прво, очигледно је да конвенционални ревизорски приступ (тачка 3.1) и приступ екстерних ревизора (тачка 3.3) ни у ком случају не би могли да детектују предметну слабост система, без обзира на ниво детаљности, утрошено време и уложени напор. Једноставно, ова слабост је у потпуности изван опсега рада финансијских ревизора, већ по самој природи њиховог посла и предмета рада. Технологија је принципијелно (системски) изван њиховог видогруга – она је једноставно једна од „слепих тачака” у њиховом приступу.

Међутим, комбиновање приступа конвенционалне ревизије са технолошким приступом (тачка 3.3.2) као и приступ у којем се утврђује усклађеност са ISO стандардима (тачка 3.4) у принципу су имали могућност да открију ову и овакву слабу тачку. Конкретно, оба ова приступа захтевају да се прегледа процес управљања променама (видети контролу ОК.2 у тачки 3.3.2). Ако прате оквири које поставља COBIT или спроведу доследну проверу усклађености са ISO/IEC 27001, могли бисмо очекивати да ће то довести ревизоре до открића ове слабости. И један и други приступ обухватају област управљања информатичким средствима, оперативним процедурама и све друге релевантне техничке и организационе аспекте управљања информатичком безбедношћу. Ипак, ревизори нису открили предметну слабост. Једноставно, ни COBIT ни ISO/IEC 27001 нису у могућности (нити су тако замишљени) да упуте организацију у све детаље њихове имплементације. Ма колико да се у том погледу ишло у детаље, оба оквира остају на

широко постављеним препорукама и вишем нивоу општости од онога који конкретна имплементација захтева. Подразумева се да имплементациони детаљи треба да буду даље разрађени у актима којима конкретне организације покривају све своје специфичности (политике, компанијски стандарди, процедуре, упутства итд). Организациона структура, величина организације, подручје пословања, стратешки и други пословни циљеви и низ осталих специфичности нужно остају изван оквира *COBIT* и *ISO/IEC 27001*. У противном, ови оквири би изгубили своју универзалну применљивост.

У конкретном случају, пропуст је настао хронолошки пре успостављања функције за контролу системских промена, односно приликом самог успостављања те функције. У том тренутку није обављена одговарајућа примопредаја власништва над информатичким системима и средствима нити је извршена подела (прерасподела) улога, тако да је у систем за контролу промена примљен и сервер базе података који нема власника. По својој природи, ова примопредаја и подела улога представља једнократни, нерепетитивни поступак, тако да је ревизија по било којем од ова два оквира (*COBIT* и *ISO/IEC 27001*) могла пропуст у поступку да установи једино ако би била обављена у време када је пропуст и учињен. Међутим, пошто је ревизија вршена много касније, када је процес контроле системских промена био већ устаљен, ревизори су могли једино да установе да овај контролни процес постоји, да је правилно постављен и да исправно функционише.

Осим тога, ни један од ова два оквира не бави се одговором на питање у каквом је стању и да ли исправно функционише сама технологија на коју се примењени процес контроле промена односи. За тај ниво контроле организација мора сама да се побрине. Посебно значајан налаз је да се за ефикасну ревизију тог нивоа контроле није довољно задржати на општим оквирима које дају *COBIT* и *ISO/IEC 2700*. Као што је студија случаја показала, технолошка ревизија је била у могућности да открије предметну слабост тек када се упустила у најситније техничке детаље имплементације, конфигурације и функционисања система. Изложени пример јасно показује (што је био и циљ ове студије случаја) да је ревизију технологија неопходно проширити знањима и вештинама из области техничких контрола, односно да технолошка ревизија мора да буде отворена за интеграцију најразличитијих знања, техника и алата – чак и из области које нису блиске традиционалном схватању ревизије – као што су етичко хаковање, експериментално манипулисање системима, контролисани напади, тестови на пробој и слично.

4. ДИСКУСИЈА

Овај део рада је замишљен као осврт на неколико тема и питања која су остала отворена, која подстичу на расправу и дискусију и која траже одговоре, иако до њих можда и није нужно нити је могуће доћи унутар оквира овог рада.

4.1. ДЕФИНИЦИЈА ТЕХНОЛОШКЕ РЕВИЗИЈЕ

У делу 2.3.2 (*Дефиниција технолошке ревизије*) наведен је став из *Information Technology Auditing: An Evolving Agenda* (аутор: *Jagdish Pathak*) [26], као пример покушаја да се дефинише технолошка ревизија. Овде ћемо поновити овај навод, како бисмо се осврнули на неке проблеме које отвара не само ова дефиниција, већ и сваки други покушај дефинисања ревизије у примени и коришћењу технологија уопште.

„Ревизија информационих технологија је процес прикућвања и процене (евалуирања) доказа о томе да ли један информациони систем:

- штићи средства и имовину,*
- одржава интегритет података,*
- ефективно достиже циљеве које је поставила организација и*
- ефикасно користи ресурсе.”*

Захтеви које мора да испуни информациони систем, и чија је испуњеност предмет ревизорског оцењивања у овом ставу се експлицитно набрајају. Међутим, набројани захтеви се не налазе у истом нивоу општости. Набрајање „осцилује” између општег и посебног – на пример појам „циљева које поставља организација” је општији од остала три. Осим тога, он их обично и обухвата, тј они су већ у њему садржани (набројани захтеви би требало да буду међусобно ортогонални, тј да се ниједан од њих не може „разложити” на неке од осталих). Следећи проблем је тзв непотпуно набрајање – помиње се интегритет података али не и тајност или расположивост (та три заједно представљају основне принципе безбедности података, који као такви представљају такође обавезан предмет ревизије). Такође, помиње се „ефективно” достизање циљева (као да ревизију не интересује ефикасност или економичност), непрецизно се захтева да (ИС) „штити” имовину (не види се коју имовину, како и од чега је штити) итд. На крају, ревизија се дефинише као ревизија *технолоџија* али се из исте дефиниције види да се она односи на *системе*.

Онај ко претендује на то да уведе дефиницију ревизије технологија неминовно се сусреће са неколико озбиљних проблема у погледу захтева које једна таква дефиниција треба (мора) да испуни. Прво, ту је питање да ли је технолошка ревизија обавезно интерна или може (или мора?) да буде екстерна. Даље, ту је питање назива – ревизија *система* или ревизија *технолоџија*. Затим, кад је реч о називу – ревизија система или технологија, али каквих – *информационих, информационих и комуникационих, савремених*, или просто (без икаквог придева) *ревизија система* односно *ревизија технолоџија*? Ово нису само формална, реторичка питања. Њихов значај је велики јер добра дефиниција поставља добар оквир у којем се даље могу разрађивати циљеви, место, улога и одговорности, поступци, технике итд.

Ако се ослонимо на (претходно усвојену) дефиницију интерне ревизије (видети: 2.2.1.) и покушамо из ње да изведемо за један степен општости нижу дефиницију, такву да третира технолошку ревизију као део опште ревизије, добили би следећу формулацију:

„Технолошка ревизија је посебна област ревизије која даје савете и пружа уверења са циљем да увећа вредност и унапреди начин примене и коришћења информационих и комуникационих технологија унутар једне организације. Она помаже организацији у постизању њених циљева тако што систематичним и дисциплинованим приступом, независно и објективно евалуира (процењује) и унапређује процесе управљања ризиком, контроле и управљања информационих и комуникационих технологија и на њима заснованих система у организацији.”

Овако формулисана дефиниција строго прати структуру и садржај дефиниције коју даје ИА (2.2.1.) с тим што се сужава на област контроле и управљања само оних процеса који се тичу примене и коришћења информационих и комуникационих технологија у организацији. При томе, избегнуто је навођење да ли се ради о интерној (или о екстерној) ревизији.

Уколико се ограничимо искључиво на интерну ревизију, дефиниција би се могла додатно скратити, уклањањем референци на опште карактеристике (давање савета и уверења, објективност, независност, систематичност и дисциплина) и увођењем генералне референце на претходно дефинисану интерну ревизију (као на шири појам, први виши по нивоу општости):

„Технолошка ревизија је посебна област интерне ревизије која процењује и унапређује процесе управљања ризиком, контроле и управљања у области примене и коришћења информационих и комуникационих технологија и на њима заснованих система у организацији.”

На крају, ако се сложимо да је у области технологија једина разлика између интерне и екстерне ревизије у припадности организационој структури која је извршава, онда се горња дефиниција може свести на следеће (простим избацивањем атрибута „интерна”):

„Технолошка ревизија је посебна област ревизије која процењује и унапређује процесе управљања ризиком, контроле и управљања у области примене и коришћења информационих и комуникационих технологија и на њима заснованих система у организацији.”

Међутим, ова дефиниција дилему око назива само избегава, али је не разрешава. Да би се ова дилема отклонила, потребна су нека додатна разматрања, која су дата у тачки 4.2.

4.2. РЕВИЗИЈА СИСТЕМА ИЛИ РЕВИЗИЈА ТЕХНОЛОГИЈА?

Појам „информациони системи” је врло широк. Изворно, он је доста шири од појма „информационе технологије”. Наиме, он обухвата не само информационо-технолошке, већ и низ других аспеката – системски и апликативни софтвер, пословну логику спроведену кроз апликације, организационе, персоналне аспекте итд. То свакако иде у прилог избора овог назива, због чега се он, уосталом, дуго и веома много користи.

Ипак, у овом раду учињен је избор да се у називу користи реч технологија уместо речи систем. Дакле – ревизорска активност у области информатике се овде назива *ревизија технологија* а не *ревизија система*.

Да би се образложио овакав избор назива, потребно је сагледати шта се дешавало са информационим технологијама и информационим системима у времену од када је термин информациони систем ушао у употребу па до данас. У том периоду (приближно од краја осамдесетих година прошлог века на даље) издвајају се два веома значајна и глобално присутна процеса (феномена). Први је конвергенција информационих и комуникационих технологија а други је експанзија рачунарског умрежавања и појава Интернета.

Конвергенција је почела тако што су најпре рачунари уведени као средство за управљање комуникационим уређајима. Недуго затим, брзи развој довео је до тога да нисмо могли да разликујемо телефонску централу од рачунара. Даље, постало је тешко утврдити разлику између рачунарских и телекомуникационих мрежа, док данас чак и терминална опрема постаје међусобно неразлучива, ако не и сасвим иста. Савремени терминали (телефонски апарати, ПДА уређаји, преносиви рачунари итд) толико су слични међу собом да се понекад разликују само по облику и димензијама, тј по фактору форме. Они користе исте оперативне системе, исти апликативни софтвер, врло сличне хардверске компоненте (процесор, пратећи „чип-сетови” итд), па чак конвергирају и по самој својој намени - рачунари све чешће служе за „телефонирање” (*VoIP, Skype, Instant messsaging*) а телефони за пренос података, мултимедијалних садржаја, приступ Интернету и слично.

Истовремено, долази до масовног умрежавања – локалног и глобалног. Мреже одавно нису „интерна ствар” једне организације – предузећа, установе или другог ентитета који их поседује и контролише. Мреже су се повезале у глобалну мрежу – „мрежу свих мрежа” – Интернет. Пословне и приватне комуникације изашле су из оквира контроле самих учесника комуникација. Информациони системи у традиционалном смислу, дакле који су у власништву и под контролом власника, престају да буду довољни за испуњење низа пословних захтева и потреба. Пословни токови се великим делом проширују на Интернет, толико да без њега често не би ни могли да се одвијају.

Притом, Интернет није само мрежа глобалних размера. Он је и технологија, тачније скуп технологија – и то такав скуп који данас поприма значај универзалног скупа. Наиме, велики број информационих технологија које данас користимо заправо нису ништа друго до један подскуп интернет технологија. Примери за то су бројни. Апликативна решења базирана на тзв „танком клијенту”, трослојна (вишеслојна) архитектура апликација, мрежни и апликативни протоколи, мобилни код и многа друга технолошка решења која се данас срећу у локалним мрежама заправо су примери интернет технологија. У току је конвергенција информационо-комуникационих технологија и интернет технологија. Све чешће смо у ситуацији да не можемо разликовати појединачни рачунар од мреже рачунара, захваљујући концептима као што су B2B повезивање (*B2B – Business to Business*), кластеринг (*Clustering*), виртуелизација, дистрибуирано рачунарство (*Cloud Computing*) и многи други. Ови незаустављиви процеси све нас више удаљавају од традиционалне слике у којој су све информационе технологије које користимо биле део нашег информационог система – система којег поседујемо и којег контролишемо у потпуности.

Дакле, савремене организације и пословни процеси у њима данас зависе од савремених технологија у мери која увелико превазилази оквире сопствених информационих система. Према томе, ако је задатак технолошке ревизије да открије и оцени сваку сметњу у достизању циљева једне организације, она мора да се бави и информационим и комуникационим технологијама у најширем смислу, било да су оне унутар или изван информационог система дате организације.

Због свега тога, у овом раду је учињен избор да се користи назив *ревизија информационих и комуникационих технологија*, или кратко *технолошка ревизија* (тамо где је из контекста јасно о којим се технологијама ради).

4.3. ТЕРМИНОЛОШКЕ ДИЛЕМЕ: ПРИЛАГОЂАВАЊЕ НЕКИХ СТРУЧНИХ ТЕРМИНА НАШОЈ КУЛТУРИ И ЈЕЗИКУ – ОБАВЕЗНО, ПОЖЕЉНО, СУВИШНО ИЛИ НЕМОГУЋЕ?

Током израде овог рада појавило се неколико дилема око избора одговарајућих термина којима би се означили неки важни стручни појмови. О некима од њих, које се тичу назива технолошке ревизије, већ је раније дискутовано (видети: 4.1 и 4.2). Строго гледано, овај рад не мора да буде место где се расправља о језику, али је потребно дискутовати о усвојеној терминологији и употреби страних речи.

Пошто нема готових стручних речника из ове области и не постоје општеприхваћени језички стандарди за усвајање стране терминологије, преостаје да аутори у сваком појединачном случају доносе изнова исте одлуке: усвојити страни термин без превода, користити дословни превод или учинити покушај да се у српском језику пронађе најпогоднија реч која ће означити одређени појам и тако практично уведе потпуно нов стручни термин у српски језик.

Пошто је стручна литература из области технолошке ревизије код нас још увек у повоју, то овај рад може бити искоришћен и као прилика да се у интересној заједници информатичара и шире поведе дискусија о стручној терминологији, или бар о појединим терминима.

У том смислу, у овом раду је учињен напор да се, где год је то могуће, избегне употреба страних речи. У неколико примера остало је отворено питање коначног избора термина. Како се ради о веома значајним појмовима, овде их наводимо, уз одговарајуће коментаре, предлоге (ако их има) и аргументацију.

4.3.1. *Governance/Management/Control*

Енглески термин *governance* има два значења:

- именица која означава колективно управљачко тело, дакле „управа”
- глаголска именица од глагола *govern* (управљати), у значењу „управљање”

Термин *management* има следећа значења:

- именица која збирно означава руководећи кадар у некој организацији – „руководство”, „управа”, „менаџмент”

- именица која означава посао који обављају руководиоци (пословна активност менаџмента) – „руковођење” или „управљање”

Термин *control* има следећа значења:

- именица која означава способност да се утиче на нечији правац (усмерење) – „управљање”, „команда”, „превласт”, „доминација”
- именица која означава део командне табле (панела) неке справе, уређаја, возила и слично – прекидач, инструмент, полуга итд – „команда”. (као у: „пилотска кабина је била пуна разних команди”)
- придев у значењу „командни/а/о” – *control panel* – командна табла
- глагол у значењу „управљати”, „командовати”, „контролисати”, „регулисати” или „имати (држати) власт (бити у власти над неким)”
- глагол у значењу „контролисати” (вршити проверу)

Ван контекста интерне ревизије, сва три термина се најчешће преводе као „управљање”. Међутим, у контексту ревизије ова три термина (односно, у преводу само један – управљање) означавају три сасвим различита појма: управљање на нивоу највише управе (управљање типа „*noses in, fingers out*”, видети: 2.4.6), управљање на нивоу извршне управе (извршног руководства) и управљање на нивоу оперативне (непосредне) контроле. Уз то, термин *control* сам за себе означава више појмова – три главна су „управљати” (управљање, управљачки/а/о), „контрола” (као командна полуга) и „контролисати” (контрола, контролни/а/о, као проверавати).

Ако желимо да између ових појмова повучемо јасну дистинкцију, било би пожељно да их означимо различитим терминима. У противном, имаћемо појмовну конфузију, крајње непожељну у теорији и пракси било које стручне области, па тако и ревизије.

Једно решење би било да се *governance* преводи као „управа” (или највиша управа), *management* као „руководство” (руковођење) а *manage* као „руководити”, док би *control* зависно од контекста и два главна значења преводили као „управљање” (управљати, управљачки/а/о) или „контрола” (контролисати, контролни/а/о).

Тако би *Governance Control* преводили као „контроле на нивоу највише управе”, *Change Management* би било „руковођење променама”, а *Control Objectives* „управљачке смернице (или циљеви)”.

Највећи проблем са овим предлогом је што је *management* већ увећано ушао у наш језик као „управљање” (*project management, change management, risk management...*) и то у контекстима где не постоји проблем са појмовима *governance* и *control*. Такође, постоји већ утемељена наука о пословању (теорија и пракса) у којој овај термин означава један од темељних појмова и то без превођења, као „менаџмент” („менаџер”, „менаџерски”...), што се такође јако много раширило и изван контекста теорије менаџмента. Зато је тешко очекивати да би овакав предлог заживео.

У овом раду је уважена широко раширена навика и *management* је преводен као „управљање” (као и *control*), с тим да је текст конструисан тако да се избегне појава оба појма у истом контексту, како не би дошло до конфузије.

4.3.2. Firewall/Router/Switch

Једино значење термина *firewall* које можемо наћи у енглеским речницима (и то одвојено, као синтагму од две речи: *fire wall*) јесте „ватростални зид”, дакле грађевински елемент који служи да спречи ширење ватре кроз просторије у зградама у случају пожара. У колоквијалном речнику овај термин такође означава и металну преграду која у аутомобилима раздваја путничку кабину од простора за мотор.

Захваљујући лакоћи којом на енглеском говорном подручју жаргон улази у стручну терминологију, овај термин је у информатичком контексту усвојен за означавање одређене врсте уређаја за мрежну безбедност. Ови уређаји раде тако што спречавају пролаз одређених типова мрежног саобраћаја – филтрирањем на мрежном, транспортном или апликативном слоју, и то у оба смера – одлазном или долазном.

Усвојити „фајервол” као страну реч није баш срећно решење. Као прво, реч не „звучи” српски и одудара у скоро свакој конструкцији реченице. Као друго, у неким контекстима *firewall* је глагол (*are all your networks firewalled?*), што га потпуно дисквалификује за директно усвајање (било би: „фајерволисати” или „фајерволисање”).

Стога је упутно пронаћи неки наш термин који би по смислу било могуће пренети на нови појам. Један покушај (већ доста раширен) је „мрежна баријера”. Међутим, треба размотрити и друге речи, чије значење би могло бити на природан начин пренешено на конкретан појам: заклон, запрека, и сл. Тако на пример, иако није до сада коришћен у домаћој стручној литератури, термин „заклон” не само да одговара по смислу, већ се доста добро понаша у већини реченичних конструкција нашег језика (потребно је поставити мрежни заклон, да ли је ова мрежа заклоњена и сл.), са и без придева „мрежни”.

У нашем језику је већ прихваћена страна реч „рута” (не само у контексту ИТ) у значењу „пут”, „правац кретања” и сл. Међутим, реч *router* је релативно нова, сасвим ограничена на контекст мрежних технологија. У овом раду је поштован већ усвојен обичај да се користи термин „рутер” (без превода), али се такође предлаже да се размотре алтернативе, као што су „усмеривач” или „скретница”.

Слично термину *firewall*, и термин *switch* се тешко уклапа у наш језик – по „звуку” и по неким језичким променама (свиеви, свичовање) та реч једноставно одудара од остатка реченице и било би пожељно наћи јој замену.

Реч *switch* значи прекидач (измењивач, скретница). Ушла је у технички речник далеко пре експанзије рачунарских мрежа – у телекомуникацијама она означава централу (телефонску, телеграфску, *Frame Relay*, *ATM*) у којој се саобраћај комутира – проспајањем или раскидањем веза између прикључних тачака. Најближа по смислу, реч „комутатор” је такође страна, али се лакше уклапа у српски језик (већ је раније усвојена и користи се као страна реч). Међутим, сматрамо да треба размотрити реч „сабирница”. Строго говорећи, по смислу би сабирница пре била *hub* (што је такође један од мрежних уређаја), међутим пошто су „хабови” већ увелико превазиђени и замењени „свичевима” (интелигентним хабовима), то би можда „сабирница” могла да остане као термин и за нову, интелигентну генерацију „хабова” – „хабова са могућношћу комутације”.

4.3.3. Backup/Restore

Термин *backup* изворно означава подршку, појачање или замену. Међутим, у информатичком контексту она означава копирање података на одвојени меморијски уређај (на засебни медијум) у циљу заштите од њиховог губитка, као и саму ту копију.

Дакле, та копија је по мотиву за њену израду заштитна или резервна. Иако се често среће „бекап” (без превођења), термин „резервна копија” је доста широко прихваћен. Ипак сматрамо да би поред тога требало размотрити и изворну српску реч „препис”. Прво, копија је ипак страна реч (иако широко прихваћена), а друго – реч „препис” је изворно означавала потпуно исти појам који у данашње време означава реч *backup*. Наиме, супротно широком уверењу, у време пре појаве штампе, стари рукописи су ручно преписивани не (само) зато да би се постигао „тираж” (шира доступност њиховог садржаја), већ пре свега из разлога безбедности – да би се садржај драгоцених оригинала заштитио од губитка.

5. ЗАКЉУЧЦИ

Теоријски, а посебно практични део рада (студија случаја) у целини потврђују како општу тако и појединачне хипотезе које су узете као полазне тачке рада и оквир истраживања. Истовремено, постигнути су и општи (научни) и конкретни циљ овог рада.

Најзначајнији закључци који се могу извести из целокупног истраживачког рада и његових резултата и који потврђују претходни став могу се поделити у неколико целина.

5.1. ДУАЛИЗАМ И ПАРЦИЈАЛНИ ПРИСТУПИ У ТЕХНОЛОШКОЈ РЕВИЗИЈИ

Пре свега, рад је показао да у ревизорској теорији и пракси данас заиста постоји дуализам између две „школе” које паралелно егзистирају и које су у контексту рада условно назване традиционална (финансијски оријентисана) и савремена (технолошки оријентисана) ревизија. Оне су међусобно комплементарне, у пракси често и супростављене, иако уз извесна преклапања у методама и приступу. Овим је потврђена општа хипотеза, постављена на почетку (видети: 1.3. *Хипотетички оквир*).

Поред тога, показано је да су веома присутни и уски, парцијални приступи, у којима се технолошкој ревизији искључиво приступа са неког ограниченог гледишта – према организационој шеми, према подели одговорности, системској топологији, процени ризика, животном циклусу итд. Такође је закључено да је, у циљу „покривања” слабо контролисаних области, често увођење засебних, међусобно искључивих контролно-ревизорских дисциплина, као што су ревизија безбедности, ревизија усклађености, ревизија против преваре и сл. Оне међусобно слабо или никако не сарађују и, по правилу, не успевају да сагледају целину проблематике технолошке ревизије.

5.2. НЕОПХОДНОСТ ИНТЕГРАЦИЈЕ

У раду су демонстрирана ограничења, слабости и пропусти који се јављају тамо где постоји било каква искључивост у избору приступа (видети: 3. *Студија случаја*, као и 2.5.10). У том смислу, садржај рада указује на закључак да је неопходна конвергенција (интеграција) не само појединих парцијалних приступа, већ и обе „школе”, и то у једну свеобухватну целину. Иако у себи хетерогена и изразито мултидисциплинарна, овако интегрисана технолошка ревизија мора бити способна да према спољном окружењу делује јединствено и хомогено, јер само на тај начин, тесном сарадњом и координацијом свих својих компоненти, може у потпуности да испуни своју улогу и пружи пуну заштиту од технолошки оријентисаних ризика у пословним процесима предметне организације. Оптимално комбиновање теорије и праксе постојећих „школа” и свих познатих приступа представља једини начин за превазилажење индивидуалних ограничења и унапређење укупне ефикасности и ефективности технолошке ревизије. Овај закључак уједно потврђује појединачну хипотезу и основни научни циљ рада (видети: 1.3.2 и 1.4.1).

5.3. ЗНАЧАЈ ТЕХНИЧКИХ КОНТРОЛА И ОДГОВАРАЈУЋИХ СТРУЧНИХ КОМПЕТЕНЦИЈА

Даље, рад је показао велики значај техничких контрола у области третмана ризика у организацијама. С тим у вези, постављено је питање одговарајућих техничких компетенција технолошких ревизора. Показано је да сложени и софистицирани технолошки системи захтевају исто тако сложене и софистициране техничке контроле, те да су за проверу њихове адекватности и ефикасности неопходна и веома висока стручна знања.

Савремена реалност је таква да се у већини организација далеко већи пословни ризици крију у области технологија, њиховој примени и коришћењу код разних врста услуга, него што је то случај у области економије, финансија и слично. Наиме, област финансија је веома добро покривена законима, прописима, интерном регулативом, па и екстерном ревизијом, тако да је непокривени, резидуални ризик веома мали. Интерне контроле су ту строго прописане законима и професионалним стандардима. Са друге стране, савремене технологије представљају стални изазов за системе интерних контрола. Ту се нови ризици откривају са месечном динамиком (каткада и дневном), што измиче свакој правној и техничкој регулативи и захтева посвећеност и веома интензиван ангажман уско стручног особља, спремног на перманентну едукацију и усавршавање.

Један од значајнијих закључака у том смислу јесте да напредне и уско специјализоване дисциплине, као што су етичко хаковање, експериментално манипулисање системима, контролисани напади, пробојни тестови, дигитална форензика и слично неизоставно морају постати део експертског арсенала којим располаже савремена технолошка ревизија.

5.4. НЕОПХОДНОСТ ДЕФИНИСАЊА УЛОГЕ И МЕСТА ТЕХНОЛОШКЕ РЕВИЗИЈЕ

Значајни део рада је посвећен тражењу одговарајуће дефиниције технолошке ревизије, њене улоге и одговорности у организацији. Предложена је дефиниција која се наслања на опште прихваћену дефиницију интерне ревизије и која одражава све најбитније карактеристике интегрисаног концепта технолошке ревизије. Предложен је назив „ревизија информационих и комуникационих технологија”, односно „технолошка ревизија” (на оним местима где је из контекста јасно о каквим је технологијама реч). Закључак рада је да је за технолошку ревизију најповољније да се организује као део интерне ревизије, уколико таква пословна функција постоји у организацији. У организацијама чије специфичности условљавају недовољну независност ревизије или у којима интерна ревизија уопште не постоји, препоручује се коришћење услуга екстерне технолошке ревизије. У организацијама у којима је препознат такав пословни интерес (или је то законска обавеза), технолошка ревизија може бити позиционирана и у оквиру функције информатичке (или ИЦТ) безбедности, под условом да тиме није нарушен принцип независности од клијента ревизије.

5.5. СПЕЦИФИЧНА НЕЗАВИСНОСТ И ОБЈЕКТИВНОСТ

Поред општеприхваћених принципа независности и објективности који представљају основ опште (а посебно интерне) ревизије, рад указује на одређене, веома значајне, специфичности које у том погледу постоје код технолошке ревизије (видети: 2.3.4). Може се извести закључак да су код технолошке ревизије присутни додатни, нешто строжији захтеви који се морају испунити како би се задовољила ова два принципа. Рад указује на неке скривене и на први поглед тешко уочљиве везе између функције технолошке ревизије и њених клијената, како у случају интерне тако и код екстерне технолошке ревизије.

5.6. ПОТРЕБА ЗА СТРУЧНОМ ЛИТЕРАТУРОМ

У раду је препозната непокривеност технолошке ревизије одговарајућом литературом која би требало да пружи како теоријску подлогу, тако и преглед практичних искустава, савремених достигнућа у овој струци и припадајућих стандарда, стручне регулативе и препорука у свету. Закључак је да то отвара широко поље будућег деловања, те да је овим радом учињен један мали помак у том смислу, који ипак није сасвим без значаја. Између осталог, рад даје исцрпан преглед ревизорских алата, референце на најзначајније радне оквире, стандарде и препоруке, отвара дискусију о стручној терминологији, називу и дефиницијама у овој области. Такође, рад садржи и преглед значајнијих професионалних удружења и организација, најважнијих професионалних сертификата и референтне литературе, што све заједно заокружује целину која може да послужи као једно практично приручно средство које заинтересованим странама указује на најбитније правце даљег изучавања области технолошке ревизије. Овим је истовремено испуњен и један од најбитнијих циљева рада (видети: 1.4.1 и 1.4.2).

6. ПРИЛОЗИ

6.1. ДЕФИНИЦИЈЕ ИНТЕРНЕ РЕВИЗИЈЕ

Данас постоји високи степен сагласности око појма интерне ревизије – стручни кругови се углавном придржавају дефиниције коју је развио Институт интерних ревизора (*The Institute of Internal Auditors – IIA*). Ова дефиниција је резултат вишегодишњег настојања да се у што сажетијој форми изразе суштина, основне карактеристике и циљеви професије интерног ревизора. У приложеној табели дат је историјски преглед најзначајнијих дефиниција појма интерне ревизије, као својеврсна илустрација њеног еволутивног развоја. Дефиниције су дате без превода, у изворном облику, преузетом из *The Internal Auditing Handbook* (К.Н. Spencer Pickett)[29].

The Auditing Practices Board (APB) Definition 1990:	
	<i>Internal Auditing is an independent appraisal function established by management for the review of the internal control system as a service to the organisation. It objectively examines, evaluates and reports on the adequacy of internal control as contribution to the proper, economic, efficient and effective use of resources.</i>
The Institute of Internal Auditors (IIA) 1991:	
	<i>Internal Auditing is an independent appraisal function established within the organisation as a service to the organisation. It is a control that functions by examining and evaluating the adequacy and effectiveness of other controls.</i>
The Institute of Internal Auditors (IIA) New Definition 1991:	
	<i>Internal Auditing is an independent appraisal function established within the organisation as a service to the organisation. The objective of internal auditing is to assist members of the organisation and on the board in the effective discharge of their responsibilities. To this end it furnishes them with analysis, appraisals, recommendations, counsel and information concerning the activities reviewed.</i>
The Institute of Internal Auditors (IIA) Updated Definition 1994:	
	<i>Internal Auditing is an independent appraisal function established within the organisation to examine and evaluate its activities as a service to the organisation. The objective of internal auditing is to assist members of the organisation, including those in management and on the board in the effective discharge of their responsibilities. To this end it furnishes them with analysis, appraisals, recommendations, counsel and information concerning the activities reviewed. The objective includes promoting effective control at reasonable cost.</i>
IIA Standards 2004-2009:	
	<i>Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.</i>

Табела 1: Дефиниције интерне ревизије у периоду 1990-2009.

6.2. ПРОФЕСИОНАЛНА РЕГУЛАТИВА (СТАНДАРДИ, ПРЕПОРУКЕ И РАДНИ ОКВИРИ)

6.2.1. *Регулатива Института интерних ревизора (The Institute of Internal Auditors – IIA)*

a) **The Professional Practices Framework**

- Definition of Internal Auditing
- Code of Ethics
- International Standards for the Professional Practice of Internal Auditing.

б) **Global Technology Audit Guides – GTAG**

- GTAG-01: Information Technology Controls
- GTAG-02: Change and Patch Management
- GTAG-03; Continuous Auditing
- GTAG-04: Management of IT Auditing
- GTAG-05: Privacy Risks Managing and Auditing
- GTAG-06: IT Vulnerabilities Managing and Auditing
- GTAG-07: IT Outsourcing
- GTAG-08: Application Controls Auditing
- GTAG-09: Identity and Access Management
- GTAG-10: Business Continuity Management
- GTAG-11: Developing IT Audit Plan
- GTAG-12: IT Projects Auditing
- GTAG-12A: IT Projects Auditing Appendix – Audit Questionnaire

в) **Guide to the Assessment of IT Risk – GAIT**

- GAIT Methodology
- GAIT for IT General Control Deficiency Assessment
- GAIT for Business and IT Risk (GAIT-R)
- GAIT Case Study XYZ.com - Year 2
- Guide to the Assessment of IT General Controls - Scope Based on Risk (GAIT) - December 2007
- GAIT Template for Less Complex Scenario
- GAIT Template for More Complex Scenario
- Case Studies of Using GAIT for Business and IT Risk (GAIT-R) to Scope PCI Compliance

6.2.2. Регулаторна Асоцијација за ревизију и контролу информационих система (Information Systems Audit and Control Association – ISACA)

a) IS Standards, Guidelines and Tools and Techniques for Auditing and Assurance and Control Professionals

- Code of Professional Ethics
- IT Auditing Standards, Guidelines and Tools and Techniques
- IS Control Professionals Standards
 - Tools and Techniques:
 - IS Risk Assessment Measurement Procedure P1
 - Digital Signature and Key Management Procedure P2
 - Intrusion Detection Systems (IDS) Review Procedure P3
 - Virus and Other Malicious Code Procedure P4
 - Control Risk Self-assessment Procedure P5
 - Firewalls Procedure P6
 - Irregularities and Illegal Acts Procedure P7
 - Security Assessment–Penetration Testing and Vulnerability Analysis Procedure P8
 - Evaluation of Management Control Over Encryption Methodologies Procedure P9
 - Business Application Change Control P10
 - Electronic Funds Transfer (EFT) P11

б) COBIT – Control Objectives for Information and Related Technologies

Четири дела:

- Control Objectives
- Control Practices
- Audit Guidelines
- Management Guidelines

ИТ ПРОЦЕСИ (IT PROCESSES)

Домен ПО (Plan and Organize)

- PO1 Define a Strategic IT Plan and direction
- PO2 Define the Information Architecture
- PO3 Determine Technological Direction
- PO4 Define the IT Processes, Organization and Relationships
- PO5 Manage the IT Investment
- PO6 Communicate Management Aims and Direction
- PO7 Manage IT Human Resources
- PO8 Manage Quality
- PO9 Assess and Manage IT Risks
- PO10 Manage Projects

Домен АИ (Acquire and Implement)

- AI1 Identify Automated Solutions
- AI2 Acquire and Maintain Application Software
- AI3 Acquire and Maintain Technology Infrastructure
- AI4 Enable Operation and Use
- AI5 Procure IT Resources
- AI6 Manage Changes
- AI7 Install and Accredited Solutions and Changes

Домен ДС (*Deliver and Support*)

DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

Домен МЕ (*Monitor and Evaluate*)

ME1	Monitor and Evaluate IT Processes
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

6.2.3. *Стандарди Међународне организације за стандардизацију (ISO) и других стандардизационих организација*

а) Међународни стандарди ISO/IEC

- ISO/IEC 9796 Information technology — Security techniques — Digital signature schemes giving message recovery
- ISO/IEC 9797 Information technology — Security techniques — Message Authentication Codes (MACs)
- ISO/IEC 9798 Information technology — Security techniques — Entity authentication
- ISO/IEC 13888 Information technology — Security techniques — Non-repudiation Techniques
- ISO/IEC 14888 Information technology — Security techniques — Digital signatures
- ISO/IEC 10118 Information technology — Security techniques — Hash Functions
- ISO/IEC 11770 Information technology — Security techniques — Key Management
- ISO/IEC 15946 Information technology — Security techniques — Elliptic Curve Cryptography
- ISO/IEC 18014 Information technology — Security techniques — Time-stamping services
- ISO 19092-1 Financial Services — Security — Part 1: Security framework
- ISO 19092-2 Financial Services — Security — Part 2: Message syntax and cryptographic requirements
- ISO/IEC 19790 Security requirements for cryptographic modules (FIPS 140)
- ISO/IEC 24762:2008 Information technology — Security techniques — Guidelines for information
- ISO/IEC 27000 Information Security Management System Family of Standards – Introduction and Glossary
- ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management
- ISO/IEC 27005 – designed to assist the satisfactory implementation of information security based on a risk management approach (published in 2008)
- ISO/IEC 27006 – a guide to the certification/registration process (published in 2007)
- ISO/IEC 27011 – information security management guidelines for the telecommunications industry (published by ISO/IEC in 2008 and also published by the ITU as X.1051)
- ISO/IEC 17799 Information technology – Code of practice for information security management
- ISO/IEC 21827:2002 Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM®)
- ISO 9564 Banking — Personal Identification Number (PIN) management and security (in ATM and POS systems)
- ISO/IEC 15408 Common Criteria — Evaluation Criteria for Information Technology Security

- ISO/IEC 15443-1:2005 Information technology – Security techniques – A framework for IT security assurance – Part 1: Overview and framework
- ISO/IEC 15443-2 Information technology – Security techniques – A framework for IT security assurance - Part 2: Assurance methods
- ISO 15292 Information technology – Security techniques – Protection Profile registration procedures
- ISO/IEC 15446:2009 Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets
- ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation
- ISO 19092-1 Financial Services — Security — Part 1: Security framework
- ISO 19092-2 Financial Services — Security — Part 2: Message syntax and cryptographic requirements
- ISO/IEC 24762:2008 Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services
- ISO 1745 Information processing — Basic mode control procedures for data communication systems
- ISO/IEC 13335 Management of IT Security Parts 1 and 2
- BS ISO/IEC 14516:2002 Information technology – Security techniques – Guidelines for the use and management of trusted third party services
- ISO/IEC TR 18044:2004 Information technology – Security techniques – Information security incident management
- ISO/IEC 18028:2006 Information technology – Security techniques – IT network security – Part 1: Network security management

а.1) Стандарди фамилије 27000 у припреми

- ISO/IEC 27003 - an ISMS implementation guide - publication expected by the end of 2009 or early 2010
- ISO/IEC 27004 - a standard for information security management measurements
- ISO/IEC 27007 - a guideline for ISMS auditing
- ISO/IEC 27008 - a guideline for Information Security Management Auditing
- ISO/IEC 27013 - a guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- ISO/IEC 27014 - an information security governance framework
- ISO/IEC 27015 - information security management guidelines for the finance and insurance sectors
- ISO/IEC 27031 - a specification for ICT readiness for business continuity
- ISO/IEC 27032 - a guideline for cybersecurity
- ISO/IEC 27033 - IT network security, a multi-part standard based on ISO/IEC 18028:2006
- ISO/IEC 27034 - a guideline for application security

б) Амерички национални стандарди

б.1) NIST – FIPS стандарди

Ознака	Датум	Наслов
FIPS 201-1	Mar 2006	Personal Identity Verification (PIV) of Federal Employees and Contractors
FIPS 200	Mar 2006	Minimum Security Requirements for Federal Information and Information Systems
FIPS 199	Feb 2004	Standards for Security Categorization of Federal Information and Information Systems
FIPS 198-1	Jul 2008	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 197	Nov 2001	Advanced Encryption Standard
FIPS 196	Feb 1997	Entity Authentication Using Public Key Cryptography
FIPS 191	Nov 1994	Guideline for The Analysis of Local Area Network Security
FIPS 190	Sep 1994	Guideline for the Use of Advanced Authentication Technology Alternatives
FIPS 188	Sep 1994	Standard Security Label for Information Transfer
FIPS 186-3	Jun 2009	Digital Signature Standard (DSS)
FIPS 185	Feb 1994	Escrowed Encryption Standard
FIPS 181	Oct 1993	Automated Password Generator
FIPS 180-3	Oct 2008	Secure Hash Standard (SHS)
FIPS 140-3	Jul 2007	DRAFT Security Requirements for Cryptographic Modules
FIPS 140-2	May 2001	Security Requirements for Cryptographic Modules
FIPS 140-1	Jan 1994	FIPS 140-1: Security Requirements for Cryptographic Modules
FIPS 113	May 1985	Computer Data Authentication (no electronic version available)

Табела 2: FIPS стандарди

б.2) NIST – специјалне публикациије

- SP 800-126 July 31 2009 DRAFT The Technical Specification for the Security Content Automation Protocol (SCAP)
- SP 800-124 Oct 2008 Guidelines on Cell Phone and PDA Security
- SP 800-123 Jul 2008 Guide to General Server Security
- SP 800-122 Jan. 13, 2009 DRAFT Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- SP 800-121 Sept 2008 Guide to Bluetooth Security
- SP 800-120 Dec. 22, 2008 DRAFT Recommendation for EAP Methods Used in Wireless Network Access Authentication
- SP 800-118 Apr. 21, 2009 DRAFT Guide to Enterprise Password Management
- SP 800-117 May 5, 2009 DRAFT Guide to Adopting and Using the Security Content Automation Protocol (SCAP)
- SP 800-116 Nov 2008A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
- SP 800-115 Sept 2008 Technical Guide to Information Security Testing and Assessment
- SP 800-114 Nov 2007 User's Guide to Securing External Devices for Telework and Remote Access
- SP 800-113 Jul 2008 Guide to SSL VPNs
- SP 800-111 Nov 2007 Guide to Storage Encryption Technologies for End User Devices

- SP 800-108 Nov. 2008 Recommendation for Key Derivation Using Pseudorandom Functions
- SP 800-107 Feb. 2009 Recommendation for Applications Using Approved Hash Algorithms
- SP 800-106 Feb. 2009 Randomized Hashing for Digital Signatures
- SP 800-104 Jun 2007 A Scheme for PIV Visual Card Topography
- SP 800-103 Oct 6, 2006 DRAFT An Ontology of Identity Credentials, Part I: Background and Formulation
- SP 800-102 Nov 12, 2008 DRAFT Recommendation for Digital Signature Timeliness
- SP 800-101 May 2007 Guidelines on Cell Phone Forensics
- SP 800-100 Oct 2006 Information Security Handbook: A Guide for Managers
- SP 800-98 Apr 2007 Guidelines for Securing Radio Frequency Identification (RFID) Systems
- SP 800-97 Feb 2007 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
- SP 800-96 Sep 2006 PIV Card to Reader Interoperability Guidelines
- SP 800-95 Aug 2007 Guide to Secure Web Services
- SP 800-94 Feb 2007 Guide to Intrusion Detection and Prevention Systems (IDPS)
- SP 800-92 Sep 2006 Guide to Computer Security Log Management
- SP 800-90 Mar 2007 Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- SP 800-89 Nov 2006 Recommendation for Obtaining Assurances for Digital Signature Applications
- SP 800-88 Sep 2006 Guidelines for Media Sanitization
- SP 800-87 Rev 1 Apr 2008 Codes for Identification of Federal and Federally-Assisted Organizations
- SP 800-86 Aug 2006 Guide to Integrating Forensic Techniques into Incident Response
- SP 800-85 B Jul 2006 PIV Data Model Test Guidelines
- SP 800-85 A-1 Mar. 2009 PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-2 Compliance)
- SP 800-84 Sep 2006 Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- SP 800-83 Nov 2005 Guide to Malware Incident Prevention and Handling
- SP 800-82 Sep 29, 2008 DRAFT Guide to Industrial Control Systems (ICS) Security
- SP 800-81 Rev. 1 Aug. 26, 2009 DRAFT Secure Domain Name System (DNS) Deployment Guide
- SP 800-81 May 2006 Secure Domain Name System (DNS) Deployment Guide
- SP 800-79 -1 Jun 2008 Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)
- SP 800-78 -1 Aug 2007 Cryptographic Algorithms and Key Sizes for Personal Identity Verification
- SP 800-77 Dec 2005 Guide to IPsec VPNs
- SP 800-76 -1 Jan 2007 Biometric Data Specification for Personal Identity Verification
- SP 800-73 -3 Aug. 13, 2009 DRAFT Interfaces for Personal Identity Verification (4 Parts)
 - Pt. 1- End Point PIV Card Application Namespace, Data Model and Representation
 - Pt. 2- PIV Card Application Interface
 - Pt. 3- PIV Client Application Programming Interface
 - Pt. 4- The PIV Transitional Data Model and Interfaces
- SP 800-73 -2 Sept. 2008 Interfaces for Personal Identity Verification (4 parts):
 - 1- End-Point PIV Card Application Namespace, Data Model and Representation
 - 2- End-Point PIV Card Application Interface
 - 3- End-Point PIV Client Application Programming Interface
 - 4- The PIV Transitional Data Model and Interfaces
- SP 800-72 Nov 2004 Guidelines on PDA Forensics
- SP 800-70 Rev. 1 Sept. 19, 2008 DRAFT National Checklist Program for IT Products--Guidelines for Checklist Users and Developers
- SP 800-70 May 2005 Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developer

- SP 800-69 Sep 2006 Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist
- SP 800-68 Rev. 1 Oct. 2008 Guide to Securing Microsoft Windows XP Systems for IT Professionals
- SP 800-67 1.1 May 2008 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
- SP 800-66 Rev 1 Oct 2008 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- SP 800-65 Rev. 1 July 14, 2009 DRAFT Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (CPIC)
- SP 800-65 Jan 2005 Integrating IT Security into the Capital Planning and Investment Control Process
- SP 800-64 Rev. 2 Oct 2008 Security Considerations in the System Development Life Cycle
- SP 800-63 Rev. 1 Dec. 12, 2008 DRAFT Electronic Authentication Guideline
- SP 800-63 Version 1.0.2 Apr 2006 Electronic Authentication Guideline
- SP 800-61 Rev. 1 Mar 2008 Computer Security Incident Handling Guide
- SP 800-60 Rev. 1 Aug 2008 Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices
- SP 800-59 Aug 2003 Guideline for Identifying an Information System as a National Security System
- SP 800-58 Jan 2005 Security Considerations for Voice Over IP Systems
- SP 800-57 Part 3 Oct 24, 2008 DRAFT Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance
- SP 800-57 Mar 2007 Recommendation for Key Management
- SP 800-56 B Dec. 10, 2008 DRAFT Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography
- SP 800-56 A Mar 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
- SP 800-55 Rev. 1 Jul 2008 Performance Measurement Guide for Information Security
- SP 800-54 Jul 2007 Border Gateway Protocol Security
- SP 800-53 Rev. 3 Aug 2009 Recommended Security Controls for Federal Information Systems and Organizations
- SP 800-53 Rev. 2 Dec 2007 Recommended Security Controls for Federal Information Systems
- SP 800-53 A Jul 2008 Guide for Assessing the Security Controls in Federal Information Systems
- SP 800-52 Jun 2005 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
- SP 800-51 Sep 2002 Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme
- SP 800-50 Oct 2003 Building an Information Technology Security Awareness and Training Program
- SP 800-49 Nov 2002 Federal S/MIME V3 Client Profile
- SP 800-48 Rev. 1 Jul 2008 Guide to Securing Legacy IEEE 802.11 Wireless Networks
- SP 800-47 Aug 2002 Security Guide for Interconnecting Information Technology Systems
- SP 800-46 Rev. 1 Jun. 2009 Guide to Enterprise Telework and Remote Access Security
- SP 800-45 Version 2 Feb 2007 Guidelines on Electronic Mail Security
- SP 800-44 Version 2 Sep 2007 Guidelines on Securing Public Web Servers
- SP 800-43 Nov 2002 Systems Administration Guidance for Windows 2000 Professional System
- SP 800-41 Rev. 1 July 9, 2008 DRAFT Guidelines on Firewalls and Firewall Policy
- SP 800-41 Jan 2002 Guidelines on Firewalls and Firewall Policy
- SP 800-40 Version 2.0 Nov 2005 Creating a Patch and Vulnerability Management Program
- SP 800-39 April 3, 2008 DRAFT Managing Risk from Information Systems: An Organizational Perspective
- SP 800-38 E Aug. 17, 2009 DRAFT Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices

- SP 800-38 A Dec 2001 Recommendation for Block Cipher Modes of Operation - Methods and Techniques
- SP 800-38 B May 2005 Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
- SP 800-38 C May 2004 Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality
- SP 800-38 D Nov 2007 Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
- SP 800-37 Rev. 1 August 19, 2008 DRAFT Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach
- SP 800-37 May 2004 Guide for the Security Certification and Accreditation of Federal Information Systems
- SP 800-36 Oct 2003 Guide to Selecting Information Technology Security Products
- SP 800-35 Oct 2003 Guide to Information Technology Security Services
- SP 800-34 Jun 2002 Contingency Planning Guide for Information Technology Systems
- SP 800-33 Dec 2001 Underlying Technical Models for Information Technology Security
- SP 800-32 Feb 2001 Introduction to Public Key Technology and the Federal PKI Infrastructure
- SP 800-30 Jul 2002 Risk Management Guide for Information Technology Systems
- SP 800-29 Jun 2001 A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2
- SP 800-28 Version 2 Mar 2008 Guidelines on Active Content and Mobile Code
- SP 800-27 Rev. A Jun 2004 Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- SP 800-25 Oct 2000 Federal Agency Use of Public Key Technology for Digital Signatures and Authentication
- SP 800-24 Aug 2000 PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
- SP 800-23 Aug 2000 Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- SP 800-22 Rev. 1 Aug. 2008 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
- SP 800-21 2nd edition Dec 2005 Guideline for Implementing Cryptography in the Federal Government
- SP 800-20 Oct 1999 Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
- SP 800-19 Oct 1999 Mobile Agent Security
- SP 800-18 Rev.1 Feb 2006 Guide for Developing Security Plans for Federal Information Systems
- SP 800-17 Feb 1998 Modes of Operation Validation System (MOVS): Requirements and Procedures
- SP 800-16 Rev. 1 Mar. 20, 2009 DRAFT Information Security Training Requirements: A Role- and Performance-Based Model
- SP 800-16 Apr 1998 Information Technology Security Training Requirements: A Role- and Performance-Based Model
- SP 800-15 Version 1 Sep 1997 MISPC Minimum Interoperability Specification for PKI Components
- SP 800-14 Sep 1996 Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-13 Oct 1995 Telecommunications Security Guidelines for Telecommunications Management Network
- SP 800-12 Oct 1995 An Introduction to Computer Security: The NIST Handbook

6.3) NIST – архивирани FIPS стандарди

Ознака	Датум	Наслов
FIPS 201	Jun 2005	Personal Identity Verification (PIV) of Federal Employees and Contractors Withdrawn: Mar 2006/ Superceded By: FIPS 201 -1
FIPS 198	Mar 2002	The Keyed-Hash Message Authentication Code (HMAC) Withdrawn: July 2008/ Superceded By: FIPS 198 -1
FIPS 186-2	Jan 2000	Digital Signature Standard (DSS) Withdrawn: Jun. 10, 2009/ Superceded By: FIPS 186 -3
FIPS 180-2	Aug 2002	Secure Hash Standard (SHS) Withdrawn: Oct. 2008/ Superceded By: FIPS 180 -3
FIPS 171	Apr 1972	Key Management Using ANSI X9.17 Withdrawn: February 8, 2005/ Superceded By: SP 800 57
FIPS 141	Apr 1985	Interoperability and Security Requirements for Use of the Data Encryption Standard with CCITT Group 3 Facsimile Equipment Withdrawn: February 25, 2000
FIPS 139	Aug 1983	Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications Withdrawn: February 25, 2000
FIPS 112	May 1985	Password Usage Withdrawn: February 8, 2005
FIPS 102	Sep 1983	Guidelines for Computer Security Certification and Accreditation Withdrawn: February 8, 2005/ Superceded By: SP 800 37
FIPS 87	Mar 1981	Guidelines for ADP Contingency Planning Withdrawn: February 8, 2005/ Superceded By: SP 800-34
FIPS 83	Sep 1980	Guideline on User Authentication Techniques for Computer Network Access Control Withdrawn: February 8, 2005
FIPS 81	Dec 1980	DES Modes of Operation Withdrawn: May 19, 2005
FIPS 74	Apr 1981	Guidelines for Implementing and Using the NBS Data Encryption Standard Withdrawn: May 19, 2005
FIPS 73	Jun 1980	Guidelines for Security of Computer Applications Withdrawn: February 8, 2005
FIPS 65	Aug 1975	Guidelines for Automatic Data Processing Risk Analysis Withdrawn: August 25, 1995 Superceded By: SP 800-30
FIPS 48	May 1905	Guidelines on Evaluation of Techniques for Automated Personal Identification Withdrawn: February 8, 2005
FIPS 46-3	Oct 1999	Data Encryption Standard (DES); specifies the use of Triple DES Withdrawn: May 19, 2005
FIPS 41	May 1975	Computer Security Guidelines for Implementing the Privacy Act of 1974 Withdrawn: November 18, 1998
FIPS 39	Feb 1976	Glossary for Computer Systems Security Withdrawn: April 29, 1993/ Superceded By: NIST IR 7298
FIPS 31	Jun 1974	Guidelines for Automatic Data Processing Physical Security and Risk Management Withdrawn: February 8, 2005/ Superceded By: SP 800-30

Табела 3: Архивирани FIPS стандарди

в) Индустриски стандарди у приватном власништву

- RSA (The Rivest Shamir Adleman algorithm)
- Публикације Форума за информатичку безбедност (*ISF - Information Security Forum*)

- ISF Standard of Good Practice
- FIRM – Fundamental Information Risk Management
- IRAM – Information Risk Analysis Methodology
- Security Healthcheck
- Information Security Benchmark Tool
- Security Management Diagnostic
- Return on Security Investment
- The ISF Security and Legislation Database
- Policy Database

Публикације Форума за информатичку безбедност доступне су само члановима Форума, са изузетком Стандарда добре праксе који је јавно доступан

г) Немачки државни стандарди, упутства и друге публикације (BSI – *Bundesamt für Sicherheit in der Informationstechnik*)

- IT Baseline Protection Catalogs (IT-Grundschatz Catalogs)
- BSI-Standard 100-1: Information Security Management Systems
- BSI-Standard 100-2: IT-Grundschatz Methodology
- BSI-Standard 100-3: Risk Analysis Based on IT-Grundschatz
- Information security audit (IS audit) - A guideline for IS audits based on IT-Grundschatz
- A Penetration Testing Model

6.3. ПРОФЕСИОНАЛНА УДРУЖЕЊА И ДРУГЕ ОРГАНИЗАЦИЈЕ ОД ЗНАЧАЈА ЗА ОБЛАСТ ТЕХНОЛОШКЕ РЕВИЗИЈЕ И ИНФОРМАТИЧКЕ БЕЗБЕДНОСТИ

- American Institute of Certified Public Accountants (AICPA) - www.aicpa.org
- American National Standards Institute (ANSI) - www.ansi.org
- American Society of Industrial Security (ASIS) - www.asisonline.org
- Association of Credit Union Internal Auditors - www.acuia.org
- Association of Certified Fraud Examiners (ACFE) - www.cfenet.com
- Association of Information Technology Professionals (AITP) (ex Data Processing Management Association) - www.aitp.org
- Australian Accounting Research Foundation (AARF) - www.aarf.asn.au
- BBBOOnline, Inc. - www.bbbonline.com
- Bundesamt für Sicherheit in der Informationstechnik (BSI) - www.bsi.bund.de
- Business Software Alliance (BSA) - www.bsa.org
- Canadian Institute of Chartered Accountants (CICA) - www.cica.ca
- Certified Practising Accountants of Australia (CPAA) (ex Australian Society of Certified Practising Accountants) - www.cpaonline.com.au
- Computer Crime & Intellectual Property Section (CCIPS) - www.cybercrime.gov
- Computer Emergency Response Team (CERT) - www.cert.org
- Computer Incident Advisory Capability (CIAC) - www.ciac.org/ciac/
- Computer Security Institute (CSI) - www.gocsi.com
- Credit Union Internal Auditors Association (CUIAA) - www.cuiaa.org
- Critical Infrastructure Assurance Office (CIAO) - www.ciao.gov
- Defense Information Systems Agency (DISA) - www.disa.mil
- Disaster Recovery Institute International (DRII) - www.drii.org
- Electronic Frontier Foundation - www.eff.org
- Federal Computer Incident Response Center (FedCIRC) - www.fedcirc.gov
- Federal Financial Institutions Examination Council (FFIEC) - www.ffiec.gov
- Foundstone, Inc. - www.foundstone.com

- High Tech Crime Investigators Association (HTCIA) - www.htcia.org
- Information Systems Audit and Control Association (ISACA) (ex Electronic Data Processing Auditors Association [EDPAA]) - www.isaca.org
- Information Systems Security Association (ISSA) - www.issa-intl.org
- Information Technology Association of America (ITAA) - www.ita.org
- Institute of Chartered Accountants in Australia (ICAA) - www.icaa.org.au
- Institute of Chartered Accountants in England & Wales (ICAEW) - www.icaew.co.uk
- Institute of Electrical and Electronics Engineers (IEEE) - www.ieee.org
- Institute of Internal Auditors (IIA) - www.theiia.org
- Interagency Operations Security (OPSEC) Support (IOSS) - www.ioass.gov
- International Criminal Police Organization (Interpol) - www.interpol.int
- International Federation of Accountants (IFAC) - www.ifac.org
- International Information Systems Security Certification Consortium, Inc. - www.isc2.org
- International Organization for Standardization (ISO) - www.iso.org
- Internet Corporation for Assigned Names and Numbers (ICANN) - www.icann.org
- Internet Engineering Task Force (IETF) - www.ietf.org
- Internet Society (ISOC) - www.isoc.org
- MIS Training Institute - www.misti.com
- National Infrastructure Protection Center (NIPC) - www.nipc.gov
- National Institute of Accountants - www.nia.org.au
- National Institute of Standards and Technology (NIST) - www.nist.gov
- National Security Agency/Central Security Service (NSA/CSS) - www.nsa.gov
- National Security Institute (NSI) - www.nsi.org
- New Technologies, Inc. (NTI) - www.forensics-intl.com
- Office of Foreign Assets Control (OFAC) - www.treas.gov/ofac
- Project Management Institute (PMI) - www.pmi.org
- RSA Data Security, Inc. - www.rsasecurity.com
- SANS (System Administration, Networking and Security) Institute - www.sans.org
- Software & Information Industry Association (SIIA) (ex Software Publishers Association [SPA]) - www.spa.org
- TruSecure Corporation (ex International Computer Security Association [ICSA]) - www.trusecure.com
- TRUSTe - www.truste.org
- USENIX (Advanced Computing Systems Association) - www.usenix.org
- VeriSign, Inc. - www.verisign.com
- World Information Technology and Services Alliance (WITSA) - www.witsa.org
- World Wide Web Consortium (W3C) - www.w3c.org

6.4. ПРОФЕСИОНАЛНИ СЕРТИФИКАТИ ОД ЗНАЧАЈА ЗА ОБЛАСТ ТЕХНОЛОШКЕ РЕВИЗИЈЕ И ИНФОРМАТИЧКЕ БЕЗБЕДНОСТИ

- CIA – Certified Internal Auditor (IIA)
- CISA – Certified Information Systems Auditor (ISACA)
- CISSP – Certified Information Systems Security Professional (ISC2)
- CISM – Certified Information Security Manager (ISACA)
- CFA – Certified Fraud Examiner (ACFE)
- CBCP - Certified Business Continuity Professional (DRII)
- CCSA - Certification in Control Self – Assessment (IIA)
- GSEC - GIAC Security Essential Certification (SANS Institute)
- GPEN – GIAC Penetration Testing Certification (SANS Institute)
- GSNA - GIAC System and Network Auditor
- ISO 27001 ISMS Lead Auditor (ISO/IEC)

7. РЕФЕРЕНЦЕ И ЛИТЕРАТУРА

- [1] BSI, *Study: A Penetration Testing Model*, BSI – Bundesamt für Sicherheit in der Informationstechnik, 2005.
- [2] BSI, *IT Baseline Protection Catalogs (IT-Grundschutz Catalogs)*, BSI – Bundesamt für Sicherheit in der Informationstechnik, 2005.
- [3] Cangemi P.M, Singleton T, *Managing the Audit Function: A Corporate Audit Department Procedures Guide, Third Edition*, John Wiley & Sons, 2005.
- [4] Cascarino R, *Auditor's Guide to Information Systems Auditing*, John Wiley & Sons, 2007.
- [5] Champlain J.J, *Auditing Information Systems, Second Edition*, John Wiley & Sons, 2003.
- [6] Coderre D, *Internal Audit – Efficiency through Automation*, John Wiley & Sons, 2009.
- [7] COSO, *Enterprise Risk Management – An Integrated Framework*, COSO, 2001.
- [8] COSO, *Internal Control – An Integrated Framework*, COSO, 2004.
- [9] Davis C, Schiller M, Wheeler K, *IT Auditing: Using Controls to Protect Information Assets*, McGraw-Hill, 2007.
- [10] Gallegos F, Manson P.D, Senft S, Gonzales C, *Information Technology Control and Audit, Second Edition*, Auerbach Publications, 2004.
- [11] Hall A.J, Singleton T, *Information Technology Auditing and Assurance, Second Edition*, South Western, 2006.
- [12] Hunton E.J, Bryant M.S, Bagranoff N.A, *Core Concepts of Information Technology Auditing*, John Wiley & Sons, 2004.
- [13] ISACA, *CobiT v4.1 – Control Objectives for Information and Related Technologies*, ISACA, IT Governance Institute, 2007.
- [14] ISF, *FIRM – Fundamental Information Risk Management*, Information Security Forum – ISF, 2007.
- [15] ISF, *IRAM – Information Risk Analysis Methodology*, Information Security Forum – ISF, 2007.
- [16] ISF, *Standard of Good Practice*, Information Security Forum – ISF, 2007.
- [17] ISO/IEC, *ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements*.
- [18] ISO/IEC, *ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management*.
- [19] Litchfield D, *Microsoft SQL Server Passwords (Cracking the password hashes)*, NGSSoftware Insight Security Research Publication, 2002.
- [20] Moeller R.R, *Brink's Modern Internal Auditing, Sixth Edition*, John Wiley & Sons, 2005.
- [21] NIST, *SP 800-12, Oct 1995 An Introduction to Computer Security: The NIST Handbook*, NIST, 1995.
- [22] NIST, *SP 800-13, Oct 1995 Telecommunications Security Guidelines for Telecommunications Management Network*, NIST, 1995.
- [23] NIST, *SP 800-14, Sep 1996 Generally Accepted Principles and Practices for Securing Information Technology Systems*, NIST, 1996.
- [24] NIST, *FIPS 200, Mar 2006, Minimum Security Requirements for Federal Information and Information Systems*, NIST, 2006.
- [25] O'Regan D, *Auditor's dictionary : terms, concepts, processes, and regulations*, John Wiley & Sons, 2004.
- [26] Pathak J, *Information Technology Auditing: An Evolving Agenda*, Springer, 2005.
- [27] Peltier R.T, *Information Security Policies and Procedures - A Practitioner's Reference, Second Edition*, Auerbach Publications, 2004.
- [28] Senft S, Gallegos F, *Information Technology Control and Audit, Third Edition*, Taylor & Francis Group/Auerbach, 2009.
- [29] Spencer K.H.P, *The Internal Auditing Handbook*, John Wiley & Sons, 1997.
- [30] Spencer K.H.P, *The Internal Auditing Handbook, Second Edition*, John Wiley & Sons, 2003.
- [31] Spencer K.H.P, *The Essential Handbook of Internal Auditing*, John Wiley & Sons, 2005.
- [32] The IIA, *Information Technology Controls GTAG-01*, IIA, 2005.
- [33] The IIA, *International Standards for the Professional Practice of Internal Auditing*, The Institute of Internal Auditors – IIA, 2009.
- [34] The IIA, *The Institute of Internal Auditors Code of Ethics*, IIA, 2009.