ДРЖАВЕН ЗАВОД ЗА РЕВИЗИЈА
ENTI SHTETËROR I REVIZIONIT
STATE AUDIT OFFICE

ПРИРАЧНИК

ЗА ИТ РЕВИЗИЈА

Скопје, декември 2022 година

СОДРЖИНА

Кратенки

INTOSAI	International Organisation of Supreme Audit Institutions
EUROSAI	European Organisation of Supreme Audit Institutions
ISSAI	International Standards of Supreme Audit Institutions
WGITA	INTOSAI Working Group on IT Audit
IDI	INTOSAI Development Initiative
ISACA	Information Systems Audit and Control Association
COBIT	Control Objectives for Information and Related Technology
ISO	International Organization for Standardization
ВРИ	Врховни ревизорски институции
IFAC	International Federation of Accountants
ИТ	Информатичка технологија
ИС	Информациски системи
ИТ ревизија	Ревизија на информациските системи
CAATs	Computer Assisted Audit Techniques
SQL	Structured Query Language
IDEA	Interactive Data Extraction & Analysis
ACL	Audit Command Language
ПДК	Планови за деловен континуитет
КИИ	Клучни индикатори за изведба
BCP	Business continuity plan
ПДК	План за деловен континуитет
DRP	Disaster recovery plan
ПОК	План за обновување по катастрофи
ПДВ	Проценка на деловно влијание

SDLC	System Development Life Cycle
ERP	Enterprise resource planning
eGov	e-Government / електронска Влада
e-gov	e-Governance / електронско управување
m-gov	Mobile governance / мобилно управување
SCARF	System Control Audit Review File
ИЗПМ	Известување за преземени мерки

1. ВОВЕД

Следејќи ги современите текови во областа на ревизијата и развојот на информатичката технологија, Главниот државен ревизор донесе акт со кој формираше тим за изработка на Прирачник за ревизија на информациски системи (Прирачник за ИТ ревизија).

Овој Прирачник е изготвен согласно меѓународните стандарди на Врховните ревизорски институции (ISSAI), Прирачникот за ИТ ревизија од страна на Работната група за ИТ ревизија (WGITA) на INTOSAI и развојната иницијатива на INTOSAI (IDI), како и меѓународно признаените ИТ рамки меѓу кои COBIT рамката на ISACA, стандардите на Меѓународната организација за стандардизација (ISO), современите трендови како и најдобрите меѓународни и европски практики и искуства во оваа област. Прирачникот нуди сеопфатно објаснување на клучните области кои ревизорите треба да ги земат предвид додека вршат ревизија на информациски системи или ревизија во услови на ИТ опкружување.

Ревизијата на информациските системи станува една од темите на ревизија која ја вршат Врховните ревизорски институции (ВРИ) во светот. Потребата од ревизија на информациски системи или ревизија во услови на ИТ опкружување е природен одговор на сè поголемата компјутеризација на работењето на владите и субјектите од јавниот сектор. Информациските системите треба да обезбедат заштита на податоците и средствата на субјектот, како и поддршка на мисијата, финансиските и останатите деловни цели. Иако употребата на информатичката технологија доведе до подобрување на деловната ефикасност и ефективност во однос на испораката на услуги/давањето услуги, истовремено донесе и ризици и слабости поврзани со компјутеризираните бази на податоци и деловните апликации кои вообичаено го дефинираат автоматизираното работно опкружување.

Информатичката технологија се развива од едноставни системи за обработка на податоци во она што е денес - системи за собирање, складирање и пристап до огромен број на податоци. Ваквите податоци се користат при носење одлуки и управување со работните процеси во субјекти.

Впрочем, со појавата и развојот на компјутерските мрежни системи, компјутерските системи станаа информациски системи. Како одраз на ваквата еволуција, поимот „Ревизија на обработката на електронски податоци" во голема мера се замени со поимите „ИТ ревизија" и „Ревизија на информациски системи".

Со зголемувањето на инвестициите и зависноста на субјектите на ревизија од компјутеризираните системи, неопходно е ревизорот да усвои соодветна методологија и пристап за да може ревизијата да ги открие ризиците по интегритетот, злоупотребата и приватноста на податоците, и да обезбеди уверување дека се воспоставени контроли за намалување на ризиците. Во еден информациски систем, особено ако е воспоставен во опкружување со неадекватни контроли, субјектот на ревизија се соочува со бројни ризици, кои ревизорот треба да е во можност да ги идентификува. Дури и тогаш кога субјектот на ревизија вовел одредени мерки за намалување на ризикот, ревизија треба да обезбеди уверување дека се воспоставени соодветни контроли и дека истите функционираат со цел да ја минимизираат изложеноста на ризици.

2. ОПШТО ЗА ИТ РЕВИЗИЈА

2.1. ИТ ревизија

Дефиниција за ИТ ревизија

ИТ ревизијата е ревизорска активност за која не постои универзална дефиниција, затоа во праксата најчесто се користи објаснувањето на Рон Вебер, кој ја дефинира како „процес на прибирање и оценување на докази за да се утврди дали еден компјутерски систем ги штити средствата, овозможува интегритет на податоците, поттикнува ефективно остварување на организациските цели и ефикасно ги употребува ресурсите"[1]. Од наведеното произлегува дека ИТ ревизијата е проверка на имплементацијата на ИТ системите за да се обезбеди уверување дека истите ги задоволуваат потребите на субјектите без да се загрози безбедноста, приватноста, трошоците и другите значајни области од работењето, како и примена на ревизорски вештини на технолошки аспекти на процесите на работењето на еден субјект.
Ревизија на информациските системи може да се дефинира како испитување на контролите поврзани со ИТ управувани информациски системи, со цел да се идентификуваат случаи на отстапување од критериумите кои, пак, се идентификувани врз основа на видот на ревизорскиот ангажман - т.е. финансиска ревизија, ревизија на усогласеност или ревизија на успешност.

Информациски системи

Информациските системи може да се дефинираат како комбинација на стратешки, менаџерски и оперативни активности вклучени во прибирање, обработка, складирање, дистрибуција и користење на информациите и сродните технологии. Комплексноста на еден ваков информациски систем може да варира од едноставна книга во која рачно се водат записи за примање и плаќање пари, до покомплексен ИТ управуван систем, како што е системот за проценка на данок, во кој сите процеси – прибирање на податоци (на пр. даночни пријави поднесени преку онлајн веб-портал), складирање на сервери, обработка на проценка (заснована на програмирање, користејќи правила за одаточување) и информирање за одаточување, поврат и признавање на данок (во реално време или во пропишани интервали) се автоматизирани. Информатичката технологија се состои од хардвер, софтвер, комуникација и други уреди што се користат за внесување, складирање, обработка, пренесување и излез на податоци во било каква форма.

[1] Weber Ron, Information System Audit, 2011

Мандат на вршење на ИТ ревизија

Мандатот на ВРИ за вршење ревизија на ИТ системите е утврден во INTOSAI-P 1 - ISSAI 1 – Декларацијата на Лима и Упатството за ревизија на информациски системи – GUID 5100, а во поширока смисла мандатот на ВРИ за вршење на ИТ ревизија произлегува од мандатот за вршење финансиска ревизија, ревизија на усогласеност и ревизија на успешност, утврдени во ISSAI 100 - Основни принципи на ревизијата на јавниот сектор. Мандатот на Државниот завод за ревизија за вршење на ИТ ревизија произлегува од Законот за државната ревизија, според кој Државниот завод за ревизија врши ревизија на регуларност и ревизија на успешност, притоа имајќи предвид дека државната ревизија подразбира и испитување на електронските податоци генерирани од информациските системи како и нивниот интегритет (точни, сигурни и навремени).

Цели на ИТ ревизијата

Целта на ИТ ревизијата е да обезбеди разумно уверување:

- дали информациските системи продуцираат навремени, точни, целосни и веродостојни информации,
- дали е обезбедена доверливост, интегритет, достапност и веродостојност на податоците,
- дали ИТ ресурсите овозможуваат ефективно постигнување на организациските цели и
- дали ресурсите се искористуваат ефикасно.
- дали ресурсите се користат ефективно и дали релевантните општи контроли и апликациски контроли се ефективни во спречување, откривање и корекција на случаи на вишок, екстраваганција и неефикасност во користењето и управувањето со информациските системи.

Притоа, потребно е ревизорот да стекне јасно разбирање за ИТ опкружувањето во кое функционира информацискиот систем, за да биде во состојба да обезбеди адекватно осигурување за тие цели. Со ова ќе се утврди видот и опфатот на ревизијата што ќе се спроведува, така што ревизорот ќе има соодветна основа врз која ќе прави конечна проценка на ИТ опкружување.

Опфат на ИТ ревизијата

Во пракса, ИТ ревизиите најчесто се составен дел на ревизиите на финансиските извештаи (проверка на точноста и комплетноста на сметководствената евиденција и финансиските извештаи на субјектот), ревизиите на усогласеност (постапка на утврдување и оценување на усогласеноста на работењето на субјектот со законите, подзаконските акти и интерните акти) или како ревизија на успешност (теми за ИТ системите или ИТ апликациите). Без оглед на видот на ревизијата, од ревизорот се бара да ги оцени политиките и постапките на ИТ опкружувањето на субјектот на

ревизија, со цел да се обезбеди уверување дека се воспоставени соодветни контроли и механизми за примена. Утврдувањето на опфатот на ИТ ревизијата вклучува одредување на обемот на ревизорските активности, опфатот на ИТ системите и нивната функционалност, ИТ процесите кои треба да се ревидираат, локациите на ИТ системите и временскиот период кој треба да се покрие. Практично ова претставува поставување или оцртување на границите на ревизијата.

ИТ ревизорски стандарди

Вршењето на ИТ ревизија и вештините потребни за вршење на такви ревизии, се базираат на општите ревизорски принципи воспоставени со меѓународните стандарди на врховните ревизорски институции (ISSAI), кои обезбедуваат рамка за сите ревизии и ги дефинираат задолжителните услови на ревизија и се во согласност со IFPP (Рамка на професионални објави на INTOSAI).
При одредување на опфатот на прашања што треба да се обработат во секоја ревизија, ревизорите треба да ги земат предвид и стандардите на Меѓународната федерација на сметководители (IFAC), меѓународни стандарди на професионални организации за ИТ ревизија како Асоцијацијата за ревизија и контрола на информационите системи (ISACA) и стандардите на меѓународната организација за стандардизација (ISO).
Освен за ИТ ревизорските стандарди, ревизорите треба да бидат информирани и за други закони, прописи, методолошки акти, кои треба да ги имаат предвид при планирање и спроведување на ИТ ревизиите.

ИТ контроли

Контролите претставуваат комбинација на методи, политики и постапки кои за субјектите обезбедуваат разумно уверување во поглед на ефективност и ефикасност на операциите, веродостојност на финансиското известување и усогласеност со применливи закони и прописи.
ИТ контролите се поделени во две категории: општи контроли и апликациски контроли.
Општите ИТ контроли се однесуваат на општата средина во која ИТ системите се развиваат, функционираат, управуваат и одржуваат.
Општите ИТ контроли воспоставуваат рамка за севкупната контрола на ИТ активностите и даваат сигурност дека општите цели се постигнати. Тие создаваат средина во која функционираат апликациските системи и апликациските контроли. Општите контроли се спроведуваат со помош на разни инструменти, како на пример стратегии, упатства и процедури, но и со воспоставување соодветни раководни структури, особено раководењето со ИТ системите кај субјектот. Примери за општи контроли се: подготовка и спроведување на Стратегија за информациски системи и ИТ политики, стандарди, упатства за безбедност и заштита на информациите, физички контроли (пристап и опкружување), контроли на логички пристап, контроли на набавки и програмски измени, контроли на промени и контроли за обновување на систем по катастрофа.

Апликациските контроли се специфични контроли за секоја компјутеризирана апликација и се однесуваат на трансакциите и постојаните податоци. Апликациските контроли вклучуваат и проверка и потврда на влезни податоци, кодирање на податоци кои треба да се пренесат, контроли на обработка итн. Апликациските контроли се единствени за една апликација и може да имаат директно влијание врз обработката на индивидуалните трансакции. Овие контроли се користат да се обезбеди уверување дека сите трансакции се валидни, комплетни, овластени и регистрирани.

Бидејќи апликациските контроли се тесно поврзани со поодделни трансакции полесно е да се види зошто тестирањето на контролите ќе му обезбеди на ревизорот осигурување за точноста на салдото на сметката. На пример, тестирање на контролите во апликацијата за пресметка на плати, ќе му обезбеди на ревизорот осигурување за податоците во платниот список и износите на плати кај субјектот.

Ревизорите можат да извршат проценка на ИТ контролите (општите и апликациските контроли) донесени од субјектот на ревизија, со цел да се испита нивната веродостојност и доволност. Проценката може да се изврши со употреба на соодветна комбинација на следниве техники: интервју, прашалник, набљудување, истражување на чекорите на процесот, дијаграм на проток на работа (flow chart), собирање и анализа на податоци, верификација, повторна пресметка, обработка и потврда од трета страна. Опфатот на проценката на ИТ контролите може да вклучи испитување за да се утврди дали:

1. Политика за ИС е дефинирана, усвоена и соопштена
2. Структурата за управување на ИС е воспоставена и функционална
3. Попис на средствата на ИС се врши периодично и се идентификуваат барања за зголемување, замена и отстранување на истите
4. Воспоставени се и функционални процеси за споделување на инфраструктура и заеднички услуги за ИС со други јавни субјекти
5. Дефинирани, усвоени и соопштени се процеси за развој, набавка и одржување на информациски системи (вклучително и оној за управување со промени)
6. Дефинирани, усвоени и соопштени се процеси за ИТ операции (внатрешни ресурси, надворешни ресурси, договор за услуги)
7. Донесени се мерки за осигурување физичка безбедност и предвидени се физички услови за работа
8. 8) Донесени се мерки за обука и одговорност на човечките ресурси за осигурување доверливост, интегритет и достапност на информациите, како и усогласеност со барањата на политиката и структурата за управување со ИС
9. Донесени се мерки за осигурување доверливост, интегритет и достапност на различните начини и канали на комуникација
10. Донесени се мерки за управување со безбедноста на информациите
11. Донесени се мерки за управување со законската усогласеност
12. Донесени се мерки за континуитет на деловното работење и управување со поврат од катастрофи
13. Апликациските контроли донесени во рамките на секој информациски систем се соодветни и сигурни. Проценката на овие контроли може да

вклучува идентификување на значајни компоненти на апликацијата, идентификување на критичката важност на апликацијата за субјектот, преглед на достапната документација, интервју со вработени, разбирање на ризиците за апликациските контроли и нивното влијание врз субјектот, како и развој на тестови за да се испита соодветноста и веродостојноста на ваквите апликациски контроли

Според тоа, проценката на општите и апликациските контроли, може да ги вклучува политиките, процесите, луѓето и системите на субјектот на ревизија, во согласност со целите на ревизијата на ИС.
Во зависност од целта на ревизијата, ревизорите може да се фокусираат на дизајнот, имплементација и ефикасноста на работењето на контролите. Кога ревизорот врши проценка на дизајнот на контролата, може да биде доволно интервју или проверка на документирани деловни правила. Кога ревизорот врши проценка на имплементацијата на контролите, може да не е доволно да се изврши само проверка, туку да биде потребно да се спроведе анализа на контролата чекор по чекор или да се изврши анализа на податоци за да се потврди дека контролата е имплементирана како што е дизајнирана. Ако, пак, ревизорот врши проценка на оперативната ефективност на контролата, од него/неа може да се побара да тестира примерок од трансакции за да демонстрира дека контролата работела ефективно во соодветниот период.
Ревизорите, исто така, може да вршат проценка како доказите за општите контроли влијаат на природата, времето и обемот на доказите потребни за да се добие уверување за работата на апликациските контроли. Доколку ревизорот има обезбедено доволни и соодветни ревизорски докази за ефективноста на општите контроли кои го поддржуваат логичкиот пристап на вработените до ИТ системите и управувањето со промените во продукцискатa средина, тој/таа може да изведе заклучок за оперативната ефикасност на автоматизираните процедури на апликациските контроли. Ова може да се постигне со тестирање на помал примерок на трансакции, бидејќи ефективноста на општото ИТ опкружување му обезбедува на ревизорот доказ за ефективноста на апликацискатa контрола во соодветниот период. Во случај на мануелни процедури на апликациските контроли, ревизорите може ќе треба да тестираат поголем примерок што одговара на избраното ниво на доверба.

Врз основа на проценката на ИТ контролите, ревизорите можат да ги идентификуваат приоритетни области за извршување на детално тестирање, кое вклучува детално тестирање на ИТ контролите со употреба на разни компјутерски потпомогнати ревизорски техники (CAAT's) за испитување, екстракција и анализа на податоци. Ревизорите може да дизајнираат и извршат детално тестирање со цел да ги потврдат целите на ревизијата. Ревизорите можат да изберат соодветни CAAT's во зависност од на нивните барања.

Општи и апликациски ИТ контроли и нивна поврзаност

Целта на општите ИТ контроли е да овозможат правилен развој и воведување на апликации, програмски и податочни датотеки и компјутерски операции.
Креирањето и воведувањето на општите ИТ контроли може да има големо влијание врз ефективноста на апликациските контроли. Општите контроли ги обезбедуваат потребните ресурси за функционирање на апликациите и спречуваат неовластени промени на апликациите или промени во поврзаните бази на податоци.
Во пракса најчесто ревизорот специјализиран за ИТ ревизија (ИТ ревизор) ги тестира контролите од областа на технологијата, додека останатите ревизори вршат контроли на финансиските извештаи и контроли на усогласеност со законите и другите прописи. Од причина што субјектите се повеќе воведуваат автоматизација во работењето, линијата помеѓу ревизорите специјализирани за ИТ ревизија и другите државни ревизори станува се потенка. Имено, сите ревизори треба да ја осознаат природата на субјектот/програмата, кој/а треба да се ревидира (ISSAI 100). Тоа вклучува разбирање на внатрешните контроли, целите, работењето, опкружувањето, системите и процесите. Улогата на ревизорот е да ги разбере ИТ ризиците со кои се соочува субјектот на ревизија и да оцени дали спроведените контроли се соодветни за постигнување на контролната цел. Кај општите ИТ контроли ревизорот треба да го разбере опфатот на општите контроли кои се во функција, да ги оцени пропустите на раководството и свесноста на вработените за истите и да утврди колку се ефективни контролите. ISSAI 1315 укажува за важноста на контролите кај финансиското известување дури и кај помалите субјекти.
Доколку општите контроли се слаби, веродостојноста на контролите на одделни ИТ апликации значително се намалува.

Планирање на ИТ ревизии и ангажирање на ИТ ревизор

Планирањето на ревизиите во Државниот завод за ревизија се утврдува со Годишната програма за работа, која ги дефинира планираните субјекти и области, односно прашањата кои ќе бидат ревидирани во текот на годината, врз основа на критериуми за избор на субјекти и области. Усвоениот пристап на планирање на ревизиите е во согласност со меѓународно прифатените стандарди и ревизорски пракси.
При подготовка на Годишната програма за работа и доставување на предлози за ревизија, потребно е да се достават предлози и за ИТ ревизија, кои ќе бидат доставувани од Секторот за ревизија на информациските системи.
ДЗР треба да осигура може да осигурат дека ревизорскиот тим е составен од членови кои заедно се компетентни да спроведат ангажмани за ревизија на ИС со цел да се постигнат предвидените ревизорски цели.

Потребното знаење, вештини и компетентност може да се стекнат преку комбинација на обука, регрутирање и ангажирање на надворешни ресурси, согласно стратешкиот план на ВРИ.

ДЗР ВРИ може да осигурат дека тимовите за ревизија на ИС заедно имаат капацитет:

1. Да ги разберат техничките елементи на еден ИТ-управуван информациски систем, вклучително сите релевантни примери на апликации во употреба, за да може да се пристапи и да се користи ИТ инфраструктурата за ревизорскиот процес
2. Да ги разберат постојните правила, регулативи и околината во која ИТ управуваните информациски системи на субјектот работат
3. Да го разберат мапирањето на деловните процеси во програмската логика за информацискиот систем на субјектот на ревизија
4. Да применат и деловно и ИТ знаење за оценка на ризикот од рачно надминување на системската програма или конфигурација што ќе овозможи исклучителна обработка на трансакции
5. Да го оценат дизајнот и да ја тестираат ефикасноста на работењето на апликациските контроли во релевантните информациски системи
6. Да ја разберат ревизорската методологија, вклучително и релевантните ревизорски стандарди и упатства што се применуваат од страна на ВРИ
7. Да ги разберат ИТ критериумите за перформанс / усогласеност во однос на кои треба да се споредат наодите од ревизијата, вклучително и рамките за управување со ИС, како што се COBIT, ITIL, TOGAF
8. Да ги разберат техниките на ИС за собирање ревизорски докази од автоматизирани системи
9. Да ги разберат алатките за ревизија на ИС за собирање, анализа и репродукција на резултатите од таквата анализа или повторно извршување на ревидираните функции
10. Да пристапат и да ја употребат инфраструктурата на ИС за наоѓање и обезбедување на ревизорските докази
11. Да пристапат и да користат алатки за ревизија на ИС за анализа на собраните докази.

ДЗР може да разгледа различни опции за алоцирање на човечки ресурси за ангажмани за ревизија на ИС. Ова може да подразбира воспоставување на централна единица со ИТ специјалисти кои им помагаат на другите ревизорски тимови во ДЗР во спроведувањето на овие ревизии или да распоредуваат ИТ специјалисти на барање. Бидејќи бројот на преземени ангажмани за ревизија на ИС се зголемува, ДЗР може да размисли за формирање на посебна група или функција за ревизија на ИС. На оваа група може да и биде доверена одговорноста за спроведување на сите ангажмани за ревизија на ИС за ДЗР и да комуницираат со други тимови во ДЗР кои имаат претходно познавање на субјектот на ревизија, со цел брзо да добијат разбирање за функциите на ентитетот и поврзаните деловни процеси. Бидејќи технологијата сè повеќе се вметнува во информациските системи, ДЗР може да осигури сите ревизори да се стекнат со соодветни вештини за ревизија на ИС

ДЗР може да ангажираат надворешни ресурси, како на пример ИТ консултанти, договорни изведувачи, специјалисти и експерти за спроведување на ревизија на ИС, во случај на ограничени ресурсите. ВРИ може да осигурат дека таквите надворешни ресурси се соодветно обучени и сензибилизирани за насоките за професионално однесување и за процесите и производите на ревизијата на ИС што се применуваат на ВРИ, и дека нивната работа е соодветно следена преку документиран договор или договор за ниво на услуга, како и соодветна вклученост на вработените на ВРИ во фазите на планирање, извршување, известување и следење на препораките на ревизијата. Затоа на ВРИ може да им бидат потребни квалификувани и со познавања членови на тимот во институцијата за да ја следат работата на надворешните ресурси и да го спроведат придржувањето кон упатствата и договорите за ниво на услуги.

2.2. ИТ ревизија како дел од ревизијата на регуларност

Согласно ISSAI 100 Врховните ревизорски институции можат да вршат ревизија и други ангажмани по било кое прашање од значење за одговорноста на раководството и оние кои се задолжени за законско користење на јавните средства. Овие ангажмани можат да опфатат најразлични теми како на пример придржување на стандарди за внатрешни контроли, системи за планирање на ресурсите на субјектите, безбедноста на информациските системи, организација и структура, кои претставуваат посебни области од информацискиот систем и можат да бидат предмет на ревизија.

Согласно ISSAI 2315, информатичката технологија е корисна за внатрешната контрола во субјектот, бидејќи овозможува да се подобри навременоста, достапноста и прецизноста на информациите, ја олеснува нивната дополнителна анализа, ја подобрува способноста за мониторинг на спроведување на активностите во субјектот, го намалува ризикот од заобиколување на контролите и дава можност за распределба на должностите со користење на безбедносни контроли во апликациите, базите на податоци и оперативните системи.

Секоја контролна област се заснова на контролни цели кои ги воспоставува субјектот, со цел да го ублажи контролниот ризик. Улогата на ИТ ревизорот е да ги утврди специфичните ризици кај внатрешните контроли со кои се соочува субјектот на ревизија, дефинирани во ISSAI 2315.

- Потпирање на системи или апликации кои не ги процесираат точно податоците, или пак процесираат погрешни податоци, или пак и двете;
- Неовластен пристап до податоците може да резултира со уништување на податоци или неправилна промена, вклучувајќи и евидентирање на неавторизирани или непостоечки трансакции, или неточно евидентирање на трансакции;
- Можноста вработените во ИТ секторот да добијат права на пристап во системот, кои се поголеми од оние што се потребни за извршување на нивните должности, кои не се во согласност со поделбата на должности;

- Неовластена промена на податоци во базата на податоци;
- Неовластена промена на системите или апликациите;
- Неизвршување на потребни промени во системите или апликациите;
- Неправилни мануелни интервенции;
- Потенцијално губење на податоци или неможност за пристапување до потребните податоци.

Ревизорот треба да преземе активности за да се увери во веродостојноста, интегритетот и доверливоста на податоците.

Ревизијата на информациските системи (ИС) ја вреднува поставеноста и функционалноста на контролите. Целите на ревизијата на ИС треба да бидат точно дефинирани, затоа што различни цели бараат различни нивоа на вештини, техники и временски распоред и имаат различен придонес во ревизорската работа како целина. Ревизорот треба ги планира следните четири аспекти за да ја процени функционалноста на контролите:

- Го утврдува опфатот на процесите кои се потпираат на информатичка технологија преку утврдување како таа ги поддржува важните процеси на субјектот и обработката на финансиските податоци;
- Обезбедува основни информации за ИТ опкружувањето на субјектот, вклучувајќи информации за апликациите кои ги поддржуваат критичните процеси, заедно со оние со кои тие се вмрежени;
- Прави преглед на оние процеси кои се потпираат, односно користат информатичка технологија кои се сметаат дека имаат директен и важен ефект на обработката на финансиските податоци и
- Врз основа на разбирањето на процесите кои се потпираат на информатичка технологија, ја евалуира ефективноста на дизајнот на секој од главните процеси кои користат информатичка технологија и поврзаните внатрешни контроли.

Врховните ревизорски институции најчесто ИТ ревизиите ги вршат заедно со ревизијата на регуларност, односно истите се составен дел од ревизиите на регуларност. Во таков случај од ИТ ревизорот се бара да ги оцени политиките и постапките на ИТ опкружувањето на субјектот на ревизија, со цел да се обезбеди уверување дека се воспоставени соодветни контроли и механизми за примена. Утврдувањето на опфатот на ИТ ревизијата го одредува обемот на ревизорската контрола, опфатот на ИТ системите и нивната функционалност, ИТ процесите кои треба да се ревидираат, локациите на ИТ системите и временскиот период кој треба да се покрие. Практично, ова претставува дел од планот на ревизијата на регуларност.

Односот меѓу резултатите од ревизијата на контролите на информациските системи и на резултатите од другите аспекти на финансиската ревизија е индиректен. Тие имаат различни, но сродни цели. Финансиската ревизија има за цел да ја провери точноста и комплетноста на сметководствената евиденција, дали

евидентираните трансакции се точни, правилно класифицирани, евидентирани на точни датуми, односно дали финансиските извештаи се веродостојни. Ревизијата на информациските системи има за цел да процени до кој степен податоците кои се обработени во финансискиот систем и од кои произлегуваат финансиските извештаи, се веродостојни. Неуспех на системот да исполни еден или повеќе контролни цели не значи неуспех на еден или повеќе искази во финансиската ревизија или дека финансиските извештаи не се веродостојни. Тоа е само показател дека системот е повеќе ранлив отколку што е претставено, вклучувајќи и закани што можат негативно да влијаат врз веродостојноста на податоците.

За подобро да се разбере врската меѓу информациските системи и финансиската ревизија треба да се земе во предвид природата на „ризикот" кој може да влијае на компјутеризираниот информациски систем. Во овој контекст, ризикот се определува со мерење на три фактори:

- Закани - несакани настани како пожар, софтверска грешка, хакирање (или инфилтрација во системот), компјутерски вирус и други закани препознаени како опасност за информациските системи.
- Ранливости - слабости на системот кои може да се искористат од заканите за да предизвикаат штета;
- Влијанија - мерења на степенот на последиците на заканата.

Финансиските системи што покажуваат ниска ранливост на заканите што можат да го повредат интегритетот на финансиските податоци имаат помала веројатност да содржат неверодостојни податоци отколку системи кои се со голема ранливост.
Ако ревизорот не е во состојба да се увери во довербата во електронските податоци од ИТ системот на субјектот предмет на ревизија, тогаш за наведената состојба обезбедува ревизорски докази и за истото информира во извештајот. Во тој случај ревизорот може да даде препораки за надминување на утврдените состојби (ISA 315/ ISSAI 2315).
Стандардите за безбедност и контрола на информациските системи не се совршени. Премногу високо ниво на контрола (над техничките можности) е премногу скапо и обично неефикасно.
Според тоа се практикува, информациските системи да не се испитуваат посебно, туку како дел на ревизија на регуларност. Само на овој начин ревизорот може реално да го процени соодветниот контролен стандард и да го вреднува взаемното дејствување на техничките контроли и контролите на корисникот.
Општите ИТ контроли се тие кои го одржуваат интегритетот на информациите и безбедноста на податоците и обично вклучуваат контроли на: добивање системски софтвер, промена и одржување, промена на програми, безбедност на пристап (ISA 315/ ISSAI 2315).

Ревизорска програма

Ревизорската програма од Прилог 1 - Општ прашалник за критичноста на системот е почетна точка за запознавање со информациските системи во субјектот предмет на ревизија. Воедно, истата ќе се користи при вршење на ревизија на информациските системи како дел од ревизијата на регуларност или како посебен тип на ревизија на успешност за оценка на информацискиот систем.

2.3. ИТ ревизијата како ревизија на успешност

Ревизијата на успешност се фокусира на испитување дали преземените активности, програми во субјектите предмет на ревизија се извршуваат односно раководат во согласност со принципите на економичност, ефикасност и ефективност и дали постојат можности за подобрување. Успешноста се оценува во однос на соодветни критериуми, при што се вршат анализи за причините за отстапувања од критериумите или за постоењето на соодветните проблеми.

Ревизијата на информациските системи (ИТ ревизија) како ревизија на успешност е процес на прибирање и евалуација на докази за да се утврди дали информациските системи се дизајнирани да го одржуваат интегритетот на податоците, да ги заштитат средствата, да овозможат ефективно постигнување на организационите цели и ефикасна употреба на ресурсите[2].
Оттука, ефективен информациски систем го води субјектот кон постигнување на целите, додека **ефикасен информациски систем** користи минимум ресурси за постигнување на целите.

ИТ ревизијата, како ревизија на успешност, може да се врши на два начини:

- ИТ ревизија, како посебна ревизија на успешност – Во овој случај информатичката технологија е главен фокус на ревизијата. При овој вид ревизија, целта на ревизијата вклучува проучување на ИТ системите на субјектот, како субјектот работи споредено со поставените стандарди, односно дали информацискиот систем е ефективен и/или ефикасен и/или економичен.
- ИТ ревизијата како дел на ревизија на успешност - Во овој случај ИТ ревизијата ја поддржува работата на ревизијата на успешност што е фокусирана на проценка на економичноста, ефикасноста и ефективноста на одделни деловни процеси/владини програми/одделни теми.

ИТ ревизијата игра важна улога во ревизиите на успешност, бидејќи од заклучоците за функционирањето на ИТ системите се очекува ревизорот да го оцени влијанието на ИТ врз процесите/ владините програми/активности / темата предмет на ревизија.

[2] Weber, R., Information Systems Control and Audit, 1999

Целта на спроведување на ИТ ревизијата е да се евалуира компјутеризираниот информациски систем, со цел да се утврди дали системот продуцира навремени, точни, целосни, и веродостојни информации[3], како и да обезбеди доверливост, интегритет, достапност и веродостојност на податоците и почитување на релевантните правни и регулаторни услови.

2.4. ИТ ревизија како дел од друг ангажман за ревизија

ДЗР треба да осигура дека ревизорскиот тим како целина работи на интегриран начин за да се постигне главната цел на ревизијата.

За да се постигне ефективна интеграција, ДЗР мора да размисли за:

- Сеопфатно документирање на работата која треба да се изврши од ревизорите на ИС;
- Дефинирање протокол за споделување на информации помеѓу ревизорите на ИС и другите ревизори;
- Идентификување кои информациски системи и контролни цели се во рамките на опфатот на ревизијата;

2.5. РЕВИЗИЈАТА ВО УСЛОВИ НА ИТ ОПКРУЖУВАЊЕ

2.5.1. Примена на информатичката технологија во ревизорската работа

Водењето на деловните/трговските книги и изготвувањето на финансиските извештаи во субјектите претставува активност која е поврзана со користење на соодветна ИТ опрема и градење на соодветни информациски системи. Информацискиот систем кој е релевантен за целите на финансиското известување, кој го вклучува и сметководствениот систем, содржи процедури и записи дизајнирани и имплементирани со цел да овозможат:

- Иницирање, евидентирање, процесирање и известување за трансакциите на субјектот (како и за настаните и условите), како и веродостојност на поврзаните средства, обврски и капитал;
- Разрешување на неточно процесирање на трансакции, на пример, автоматизирани датотеки и процедури за расчистување на времените ставки на периодична основа;
- Процесирање и одговорност за надминување или заобиколување на контролите;
- Точен и целосен пренос на податоците од системот за процесирање на трансакции во главната книга;
- Прибирање и чување на информациите различни од трансакциите, а кои се релевантни за финансиското известување;
- Сигурност дека информациите потребни за обелоденување на применливата рамка за финансиско известување се собрани, евидентирани, процесирани, сумирани и соодветно обелоденети во финансиските извештаи;

[3] ICT Audit Guideline, The National Audit Department of Malaysia, 2001

- Само одобрени ставки претставуваат влез во системот и влезните податоци се точни и целосни;
- Сигурност дека обработката на трансакциите е целосна и аритметички точна и дека резултатите (вклучувајќи ги и генерираните податоци) се точно класифицирани и правилно запишани во базите и датотеките.
- Резултатите од обработката да се точни и целосни;
- Резултатите од обработката на податоците да се достапни само до оние за кои се наменети и
- Следење на сите преземени активности во самиот систем при што за секоја настаната измена треба да има запис за идентитет на корисникот кој ја направил изменатa, времето на изменатa, како и да постои и изменетиот целосен запис.

Имајќи ја предвид важноста, улогата и значењето на информациските системи и ИТ опремата во извршувањето на деловните процеси и подготвувањето на финансиските извештаи ревизорите имаат обврска да ги земат истите предвид при извршувањето на ревизорските активности и истовремено да ја прилагодат ревизорската работа со користење на соодветна информатичка технологија за подобрување на ревизорски активности и обезбедување ефективна ревизија.

Затоа, при изготвувањето на ревизорската програма раководителот на ревизорскиот тим потребно е меѓу другото да го испита и влијанието на информатичката технологија во ревизорските постапки, вклучувајќи ја расположливоста на податоците и очекуваната употреба на ревизорски техники поддржани од компјутери, промените во информатичката технологија и деловните процеси.

Информатичката технологија е нераскинлив интегрален дел од деловните процеси/активности на субјектите вклучувајќи ги и системите за водење на деловните/трговските книги и управувањето со информациите.

Користењето на информатичката технологија на субјектите им овозможува:

- Конзистентно да ги применуваат дефинираните деловни правила и да извршуваат комплексни пресметки во процесирање на голем број на трансакции и податоци;
- Зајакнување/подобрување на навременоста, расположливоста и точноста на информациите;
- Олеснување при дополнителна анализа на информациите;
- Подобрување на можноста за надгледување на успешноста на субјектот и неговите политики и процедури;
- Намалување на ризикот од заобиколување на контролите;
- Подобрување на можноста за поделба на должности преку имплементирање на безбедносни контроли во апликациите, базите на податоци и оперативните системи.

Предностите кои ги овозможува примената на ИТ се во директна врска со начинот на кој се имплементирани контролните активности и нивното ефективно функционирање. Од перспектива на ревизорот, контролите во ИТ системите се ефективни кога го одржуваат интегритетот на информациите и безбедноста на податоците.

Во рамките на постапките кои ревизорот ги презема за идентификување и проценка на ризиците од материјално погрешно прикажување преку разбирање на субјектот и неговото опкружување, ревизорот има обврска меѓу другото да обезбеди и разбирање за информацискиот систем и поврзаните деловни процеси, кои се релевантни за финансиското известување, вклучувајќи ги и следниве области:

- Класи на трансакции во деловните активности на субјектот, кои се значајни за финансиските извештаи;
- Постапки, како во рамки на информатичката технологија (ИТ), така и во рамки на мануелните системи, со кои трансакции се иницираат, евидентираат, процесираат, коригираат во случај на потреба, се пренесуваат во главната книга и за кои се известува во финансиските извештаи;
- Поврзаната сметководствена евиденција, поткрепувачки информации и специфични сметки во финансиските извештаи кои се користат за иницирање, евидентирање, процесирање и известување на трансакции, исправки на погрешни информации и начинот на кој се пренесуваат информациите во главната книга. Евиденцијата може да се води рачно или во електронска форма;
- Начин на кој информацискиот систем ги добива податоците за настаните и условите, освен за трансакциите, кои се значајни за финансиските извештаи;
- Процесот на финансиско известување кој се користи за изработка на финансиските извештаи на субјектот, вклучувајќи ги значајните сметководствени проценки и обелоденување;
- Контроли во врска со сметководствените книжења, вклучувајќи и невообичаени книжења кои се користат за евиденција на еднократни настани (кои не се повторуваат) или исправки.

Претходно наведеното упатува на улогата и важноста на ИТ системите за генерирање на финансиските извештаи од една страна и ревизорските активности кои треба да ги преземе ревизорот за разбирање на истите, планирање на својата активност, проценка на ризиците и извршување на потребните тестирања, известување за утврдените состојби и давање препорака за надминување на истите. Со својата работа ревизорите меѓу другото имаат обврска да обезбедат информации и податоци кои ќе дадат одговор:

- Дали информациите во системите се достапни само за овластени корисници/познато како безбедност и доверливост, и
- Дали генерираните информации во ИТ системите секогаш се точни, сигурни и навремени/интегритет.

За да се изврши претходно наведената активност ревизорите имаат обврска да ги проценат ризиците на внатрешните контроли.

Извршувањето на ревизорските активности во услови на ИТ опкружување бара од ревизорите да имаат соодветно разбирање за работењето на ИТ опремата и ИТ системите, обезбедувајќи доволно докази за потврдување на точноста на влезните/излезните податоци во/од тие системи и напуштање на сфаќањето дека компјутерите „се непогрешливи", напротив - „компјутерите го прават само она што им е зададено да го направат".
Ревизорите можат да користат ИТ во процесот на планирање, извршување и известување, со цел да се намалат повторливите административни задачи и да ја направи ревизорската работа поефикасна. На тој начин повеќе од ревизорското време може да се посвети на ефективна ревизорска работа, зголемувајќи го квалитетот и продуктивноста на ревизорскиот процес.
Некои од општите начини на кои ИТ може да се користи за поддршка на ревизорската работа се:

- Користење на пакети за канцелариско работење за презентирање на нивните резултати и издавање на извештаи (MS Office);
- Вршење на онлајн истражување или онлајн пристапување кон ревизорски ресурси како што се ревизорски стандарди;
- Користење на електронски системи за доставување на прашалници за да се добие брз и целосен одговор од субјектите, на пример за да помогне во ревизорските истражувања.
- Развивање на свои сопствени пакети за планирање и управување со ресурси за да помогнат во подготовка и вршење на ревизијата. Тие пакети може да опфатат способност за евидентирање и прегледување на ревизорската работа електронски, со што се намалува количината на документите во хартиена форма кои ревизорите ги произведуваат, а одговорните лица треба да ги прегледаат. Овие пакети може исто така да опфатат модули за ревизорско планирање, евиденција на контролни активности, автоматско продуцирање на извештаи од работни белешки и следење на ревизорски препораки.

Предности во користењето на ИТ во процесот на поддршка на ревизорската работа:

- Промовирање на доследна употреба на стандардни методологии;
- Зголемена продуктивност (помалку време на подготвување на рутинската документација);
- Лесна за употреба (често изградена на стандардни пакети во општа употреба);
- Побрз увид во ревизорската документација;
- Употреба на документи од минати години за последователни ревизии;
- Достапност на податоците и намалени трошоци за складирање.

Во исто време ревизорите можат да користат ИТ со цел директно да си ја олеснат ревизорската теренска работа или за тестирање, на следните начини:

Анализирање на податоци
Анализата на податоци е важен дел од ревизорскиот пристап. Соодветната анализа може да поткрепи голем број ревизорски техники, од кои најочигледна е техниката на аналитички процедури. Овој вид анализа може да се врши било со користење на софтвер за стандардни табеларни прикази, на пример во рамките на Excel има многу „ревизорски" функции, или користење на програми посебно дизајнирани за користење од страна на ревизорите (ИДЕА софтвер).

Индексирање на ризици
Индексирањето на ризици се врши со составување на база на податоци на активности кои може да се ревидираат и со користење на софтвер за утврдување на степенот на ризик од страна на ревизорот на различните идентификувани активности. Ова може да се направи и со користење на генерички софтвер, посебно дизајнирани самостојни пакети за планирање, или модул за планирање на општ софтверски систем за ревизија.

Пребарување на податоци (Data retrieval)
Една од најопштите употреби на ИТ во процесот на ревизија е користењето на пребарување на податоци и екстракција за натамошна анализа. Некои од сметководствените системи за финансии и управување имаат вградени пакети за анализа на податоци и генератори на извештаи кои можат да бидат искористени од ревизорите, а алтернативно можат да се користат и специјални софтверски пакети.

Предности во користењето на ИТ во процесот на извршување на ревизорската функција се:

- Зголемена покриеност на тестирањето
  - Брзина и точност на компјутеризираното тестирање.
  - Подобрена големина на примерокот.
- Зголемување на опфатот
  - Може да овозможи тестирање кое поинаку би било технолошки или логистички невозможно.
- Брзина на обработката
- Флексибилност на параметрите
  - Брзината со која може да се изврши тестирањето овозможува лесно пречистување и ре-конфигурација на параметрите на тестирањето.
- Економична употреба на ревизорското време
- Независен пристап до податоците
  - Ревизорот не зависи повеќе од посредниот пристап преку корисниците или ИТ одделот на субјектот.

2.5.2. Примена на Компјутерски потпомогнати ревизорски техники - Computer Assisted Audit Techniques (CAATs)

Во време во кое секој субјект има најмалку еден процес во своето работење кој е делумно или целосно компјутеризиран, контролата на истиот од страна на ревизорите треба да биде фокусирана и кон контрола на компјутерскиот систем кој се користи. Имајќи во предвид дека најчесто се работи за покомплексни системи со значителен број на операции, токму Компјутерски потпомогнатите ревизорски техники (во понатамошниот текст CAATs) доаѓаат до израз во обезбедувањето на достатни и соодветни ревизорски докази за поткрепа на ревизорското мислење во делот на оценката на контролата на компјутерскиот систем.

CAATs претставуваат компјутерски базирани алатки, со чија помош ревизорот извршува низа автоматизирани тестови за евалуација на компјутерскиот систем на субјектот или на електронските податоци. CAATs техниките се многу корисни, особено кај контролата на субјекти кои имаат значителен број на електронски записи во базата на податоци врз која се врши контролата.
За разлика од останатите ревизорски техники (при овој вид контрола, особено рачните методи на тестирање), CAATs обезбедуваат повисоко ниво на сигурност поради тоа што:

- може да се направи темелна анализа на клучни сметководствени делови од системот,
- може да се опфатат и целосно обработат огромен број податоци, за кусо време и со релативно мал напор,
- тестовите можат лесно да се повторат врз различни бази на податоци,
- тестовите се флексибилни (се менуваат зависно од внесените параметри),
- тестовите генерираат документација која е поткрепа за ревизорскиот наод.

Исто така, ресурсите за вршење ревизија (време, луѓе, средства) можат да се искористат оптимално.

Со оглед дека субјектите предмет на ревизија ги компјутеризираат главните работни процеси, CAATs наоѓаат сè поголема примена и во ревизијата на регуларност и во ревизијата на успешност. Неретко, CAATs се основа и за обезбедување на форензички докази во случај на финансиска проневера или друг финансиски криминал.

Целите на ревизијата остануваат истите – CAATs се само алатки што му олеснуваат на ревизорот да ги исполни ревизорските цели. Според тоа, пред да започне со употреба на CAATs во текот на ревизијата, ревизорот/тимот треба да одговори на следниве прашања:

- Кои се целите на ревизијата?
- Какви податоци се потребни, за да се тестираат овие цели?

- Какви податоци поседува субјектот на ревизија?
- Каква е можноста за манипулација на податоците од страна субјектот? Кои контролни мерки треба да се применат за да се утврди евентуална манипулација?
- Дали податоците се во соодветен формат? Ако не, дали може податоците да бидат обезбедени во соодветен формат?
- Кои видови CAATs треба да се користат? Кои се специфичните предности и недостатоци?
- Дали тестовите ќе можат да се искористат и за други наредни ревизии кај субјектот или кај други субјекти?
- Дали системот кој се проверува е со висок ризик / висок приоритет?
- Дали се работи за клучен систем за работење?
- Дали трансакциите во системот се онлајн и/или во реално време?
- Дали CAATs техниките ќе повлечат дополнително време и трошоци?

Исто така, ревизорот треба да биде запознаен со:

- Организациската поставеност и работењето на субјектот
- ИТ системот кој е предмет на ревизија
- Работењето на ИТ системот, и тоа од аспект на:
  - Структурата на базата на податоци
  - Датотеките / табелите во базата
  - Релационата поврзаност во базата
  - Влезните и излезните податоци
  - Извештаите генерирани од системот.

Откако ќе ги добие одговорите, ревизорот/тимот ќе може да донесе одлука дали да користи CAATs за дадената ревизија и која од CAATs е најсоодветна за истата.

Видови CAATs

Според функцијата, CAATs можеме да ги поделиме во две основни групи:

- CAATs кои се користат за контрола на веродостојноста на процесите и програмите (софтверска анализа), и
- CAATs кои се користат за контрола на веродостојноста на податоците / базите на податоци (податочна анализа).

Треба да се напомене дека ретко кој имплементиран ИТ систем денес ја нема опцијата за водење на системски дневник на најави во системот (апликацијата). Овие системски дневници (популарно наречени системски логови) се дел од самата база или пак се водат во посебна датотека. Анализата на истите, му овозможува на ревизорот идентификување на неовластен кориснички пристап или погрешно најавување и преземање понатамошни анализи.

Софтверската анализа во принцип бара добро познавање на програмските јазици и програмирањето во целина, односно од ревизорот бара да поседува повисоко ниво на соодветна ИТ експертиза. Имајќи го предвид горенаведеното, ваквата анализа најчесто се применува од страна на ИТ ревизори и тоа како дел од ревизиите на успешност. Обично, софтверската анализа се користи за системи и апликации кои се од суштинско значење и каде проверката на контролите е од особено значење за оценка на истите.

Податочната анализа бара познавање од алатките кои се користат за добивање примерок и не се осврнува на системите, туку на податоците добиени од нив како производ. Затоа, таа е најчесто применувана, и соодветствува кај ревизиите на регуларност (или при обезбедувањето на форензички докази). Функциите кои се користат се лесно применливи на повеќе ревизии. Исто така, алатките за податочна анализа се корисни за анализа на онлајн трансакции и трансакции во реално време, како и за други системи со висок ризик.

На софтверскиот пазар постојат повеќе софтверски алатки и програми за вршење ревизија. Овие алатки најчесто се достапни за користење локално (на самиот компјутер) и можат да се користат за сите видови ревизија. Некои од главните функции (анализи) кои ревизорите ги извршуваат со помош на овие алатки се следниве:

1. **Пронаоѓање на невообичаени трансакции** – ревизорот може да извлече податоци од базата кои (не)исполнуваат одреден критериуми примероци кои се исклучок, со цел да се анализираат подетално. Овие исклучоци лесно можат да се воочат (изолираат од базата) со употреба на алатки за податочна анализа.
2. **Избор на примерок (семплирање)** – ревизорот извлекува примероци кои ја преставуваат целата база наречен репрезентативен примерок со помош на методи на избор на примерок имплементирани во софтверот за вршење ревизија.
3. **Проверка на двојни вредности (дупликат проверки)** – софтверите имаат вградени функционалности кои проверуваат двојни записи, двојни книжења, двојни корисници и сл. Дупликат проверките овозможуваат идентификација на грешки.
4. **Пронаоѓање „дупки" во датотеката** (gap detection) – ревизорот користи софтвер кој ги наоѓа т.н. „дупки" во секвенцијалните броеви на фактурите, во датумите, во реверсите и сл. што повторно е индикатор за слаби контроли при внес на податокот или пак индикатор за можна злоупотреба. Оваа алатка ги истакнува бројките што недостигаат во секвенци и е корисна за утврдување на трансакциите што недостасуваат или можни измами.
5. **Пресметки** – ревизорот ја користи оваа анализа со цел да ја провери точноста и доследноста на формулата која ја користи субјектот во системот, пр. при извлекување на податоци од база според даден критериум. Податоците добиени со пресметката, се споредуваат со податоците кои ги дава самиот систем на субјектот предмет на ревизија.

6. **Збир (totaling)** - се користи за да се докаже целосноста и усогласеноста со наведената износот на сметката.
7. **Период (Ageing)** - покажува преглед на исплати во тек на еден период. Периодот меѓу приемот и исплатата на трансакциите може да се мониторира.
8. **Споредба на датотеки (File Comparison)** - за различни цели како што е тестирање на усогласеност на податоци, детекција на неовластени активности или измами, вредности што недостигаат итн.
9. **Стратификација (Stratification)** - му дава на ревизорот јасна слика за вредностите во една датотека, со што се овозможува софистициран пристап на испитувањата и побрза идентификација на потенцијалните проблеми во датотеката.
10. **Виртуелно поле (Virtual Fields)** - создавање на виртуелно поле кое се користи за повторни пресметки за да се докаже точноста на излезните податоци.
11. **Анализа на Кориснички дневник настани (User Log)** - идентификување на неовластени обиди за влез и прекршување на лозинката[4].

11.User Log Analysis - identify unauthorized entry attempts and password violation

Алатки за податочна анализа

Најчесто користени алатки за податочна анализа се:

- Комерцијален софтвер за ревизија
- SQL и алатки базирани на SQL
- Microsoft Access или слични алатки
- Microsoft Excel или слични алатки

Комерцијален софтвер за ревизија_– ова е веќе развиен софтвер кој се продава како готов производ. Комерцијалниот софтвер ги задоволува најчестите ревизорски задачи и ги содржи сите стандардни тестови кои би ги извршил еден ревизор во ИТ ревизијата, кои веќе ги спомнавме погоре. Работата во софтверот е преку „user friendly" кориснички интерфејс. Типичен пример за ова се IDEA (Interactive Data Extraction & Analysis), и ACL (Audit Command Language). И двата софтвери работат под MS Windows и дозволуваат импортирање/експортирање податоци во најразличен формат.

SQL и алатки базирани на SQL – ова се софтверски алатки кои вршат пребарување според одредени критериуми, во релационата база на податоци на субјектот. Иако овој пристап звучи сличен на комерцијалниот софтвер за ревизија, од ревизорот бара познавање на SQL синтаксата и наредбите. Користењето на оваа алатка за пребарување може да доведе до следните ризици:

[4] Повеќето системи генерираат дневник на промените направени од корисникот и обиди за најавување. Оваа датотека е често едноставна текстуална датотека, која може лесно да се поврзе со програма за проверка или може да се провери со помош на сопствено развиена програма

- Ризикот од ненамерна промена, но неповратна промена на записите во базата, поради лошо програмирано SQL пребарување,
- Ризик од успорување на системот, доколку се врши комплексно пребарување на базата во реално време.

За избегнување на погоре наведените ризици се препорачува оваа алатка да се користи во тест околина.

Microsoft Access или слични алатки – претставуваат софтверски алатки кои најчесто доаѓаат како дел од апликациските пакети (Microsoft Office, Open Office). Релативно лесно се користат бидејќи бараат поедноставни програмерски знаења. Импортирањето на базата добиена од субјектот, пребарувањето и експортирањето на резултатите се релативно лесни. Како недостаток на Microsoft Access е дека не дозволува работа со бази поголеми од 2GB. Исто така, пребарувањето на базата оди многу бавно, доколку се работи за поголеми датотеки.

Microsoft Excel или слични алатки – претставуваат апликации кои доаѓаат како дел од апликациските пакети за канцелариско работење (Microsoft Office, Open Office). Со нив може да се импортираат податоци, да се филтрираат, да се пребаруваат според некои едноставни критериуми и слично. Основен недостаток е што не може да се анализира базата, а пребарувањето на датотеката оди многу бавно, доколку се работи за поголеми датотеки (табели).

2.6. Области на ИТ ревизии

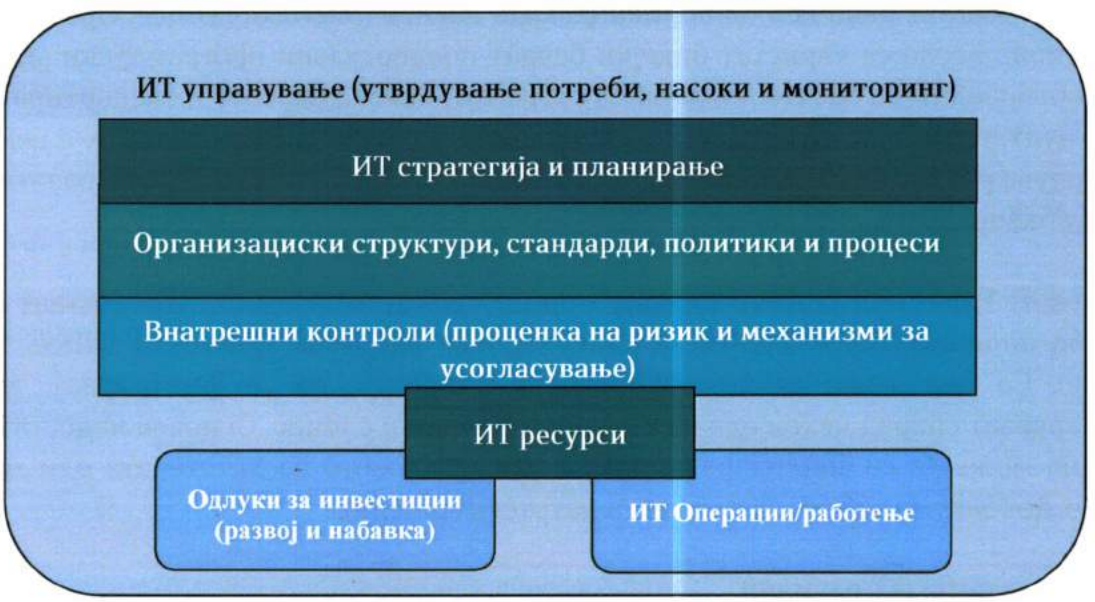
Во зависност од целта на ревизијата постојат неколку области на ревизија на информациски системи, кои се обработени во овој дел.

2.6.1. Ревизија на ИТ управување

ИТ управувањето претставува предизвик во повеќето субјекти од јавниот сектор и ВРИ сè повеќе се фокусираат на ревизија на ИТ управувањето, како дел од ИТ ревизиите. Ревизорите може да придонесат за подобрување на ИТ управувањето преку осигурување дека ИТ управувањето е составен дел на целокупниот процес на управување и преку укажување за потребата од стратегија за ИТ управување.
ИТ управувањето претставува рамка која ги опфаќа и раководи со употребата на информатичката технологија во еден субјект со цел да се осигура дека истата ги задоволува потребите на тековното работење, ги планира идните потреби и е во согласност со развојот на субјектот.
ИТ управувањето се фокусира посебно на информациските системи, нивните перформанси и управувањето со ризикот поврзан со нив. Со цел ИТ управувањето да обезбеди генерирање на додадена вредност преку инвестициите во ИТ, а ризиците да бидат минимизирани, неопходно е да се воспостави организациска

структура со добро дефинирани улоги на одговорност за информации, деловни процеси, апликации и инфраструктура.
ИТ управувањето игра клучна улога во одредувањето на контролното опкружување и ја поставува основата за воспоставување солидна пракса на внатрешни контроли и известување на функционални нивоа за надзор и проверка од страна на раководството. Постојат различни стандарди и рамки кои ги дефинираат принципите и концептите на ИТ управувањето и начин на кој субјектот може да ги спроведе истите.

На слика 2.1 е прикажана општа рамка на ИТ управување.



Неопходно е раководството да го вклучи ИТ управувањето во дефинирањето на нови или дополнителни развојни цели, за во иднина да понуди соодветни ИТ (и други) решенија. Во текот на развојот или набавка на нови решенија, ИТ управувањето осигурува дека избраните решенија ќе бидат соодветни на барањата, а потребните обуки и ресурси (хардвер, алатки, мрежен капацитет, итн.) ќе бидат достапни за имплементирање на решението. Активностите за мониторинг на овој процес, може да ги спроведува внатрешна ревизија или тим за осигурување на квалитет кои периодично ќе ги доставуваат своите извештаи до раководството.
Со извршена ревизија на успешност од страна на надворешните ревизори може да се придонесе кон подобрување на ИТ управување.

Клучни елементи на ИТ управувањето

ИТ стратегија и планирање

ИТ стратегијата претставува усогласеност помеѓу стратешките цели и целите за развој на информацискиот систем. ИТ стратешките цели се однесуваат на тековните и идните потреби на субјектот, тековниот ИТ капацитет за испорака на услуги и

потребата од ресурси[5]. Стратегијата треба да ја земе во предвид постојната ИТ инфраструктура, инвестициите, моделот на испорака и ресурсите (вклучително кадровското екипирање), како и начин на имплементација во поддршка на остварувањето на стратешките цели на субјектот.
За ревизорот е важно да ја разгледа ИТ стратегијата на субјектот со цел да го оцени нивото со кое ИТ управувањето е дел од донесување на одлуки.

Организациски структури, стандарди, политики и процеси
Организациски структури

Организациските структури се клучен елемент на ИТ управувањето во одредување на раководните и управните тела во работењето и носењето одлуки. Тие треба јасно да ги определат овластувањата за донесување одлуки и надзор над работењето.
Организацискатa структура зависи од **засегнатите страни** и **корисниците** – внатрешни и надворешни. Внатрешни корисници се раководните лица, функционалните сектори кои ги извршуваат процесите, како и лицата кои се вклучени во работните процеси. Надворешни корисници се агенциите, поединци, јавноста која е корисник на производите или услугите на субјектот други засегнати страни. Врз организациските структури влијаат и давателите на услуги– компанија, единица или лице - надворешни или внатрешни.
Соодветните организациски структури, треба да бидат пропишани од раководниот орган, при што работните задачи и одговорности за управувањето, треба да обезбедат јасна распределба на надлежности и одговорности и отчетност за важните одлуки и задачи. Тука влегуваат и релациите со давателите на ИТ услуги[6].

Организацискатa структура за ИТ најчесто се состои од следните функции:

Орган на раководење или Орган на управување кој има одговорност да врши проверка, да одобрува и да доделува финансиски средства за ИТ инвестиции.
Препорачливо е онаму каде што организацискатa ИТ структура на субјектот е посложена да се формира посебно тело за управување од област на ИТ, кое треба да биде инструмент во процесот на креирање одлуки за кои е потребна технологија за поддршка на инвестиции, но и за предлагање на набавката на таа технологија.

Раководител на организациона единица за ИТ (Chief Information Officer) треба да биде лице со соодветно искуство и одговорно за управувањето и работењето со ИТ капацитетите на субјектот. Работните задачи кои се во надлежност на ова лице се извршуваат во соработка со вработените од организационата единица, кои мораат да ги поседуваат потребните компетенции, овластувања и ресурси.

[5] Клучните елементи наведени во ова поглавје за ИТ управување се поддржани од Cobit 5 Framework и ISO 38.500 со широка употреба на нивните дефиниции и примери.
[6] COBiT 5 – Прилог Е. Мапирање на COBIT 5 со најрелевантните поврзани стандарди и рамки.

Стандарди, политики и процеси

Субјектот донесува процеси, политики и стандарди кои ги одобрува раководство. Политиките се поддржани со процедури и/или процеси кои го дефинираат начинот на кој ќе се извршува и контролира работата. Процесите/процедурите се усвојуваат од раководство за да се реализира мисијата на субјектот, а истовремено да се почитува законската регулатива. За политиките и соодветните процедури треба периодично да се информираат сите вработени во субјектот.
Одредени клучни политики кои го насочуваат ИТ управувањето се следните:

- **Политика за човечки ресурси** - ги дефинира прашањата во врска со вработување, обуки, прекин на работен однос и други активности поврзани со управувањето со човечки ресурси. Ги утврдува улогите и задолженијата на вработените, како и неопходните вештини или обуки за вработените за извршување на работните задачи. Политиката за човечки ресурси делегира надлежности и одговорности, како и нивна распределба.
- **Документација и политики за чување документи** - Документацијата за информациските системи, апликациите, работните улоги и системите за известување се важни во усогласување на ИТ операциите со стратешките цели.
- **Политика за ангажирање надворешни соработници** - Ангажирањето надворешни соработници за ИТ најчесто се користи за да помогне на раководството на субјектот да ги вложува своите напори во клучните стратешки активности. Потребата за ангажирање надворешни соработници може да биде поттикната од потребата за намалување на тековните трошоци.
- **ИТ безбедносна политика/Политика за безбедност на информациските системи** - ги утврдува барањата за заштита на информациските средства, а може да се однесува/дава упатување и на други процедури или инструменти за заштита на информациските средства. Политиката треба да биде достапна за сите вработени кои се одговорни за информацискатa безбедност, вклучително и корисниците на системите кои играат улога во чувањето информации (досиеја на вработени, влезни финансиски податоци, итн.).

Внатрешна контрола

Внатрешната контрола е процес на воведување и спроведување на систем од мерки и постапки за да се утврди дали активностите на субјектот се и остануваат доследни на одобрените планови. Доколку е потребно се преземаат неопходни корективни мерки за постигнување на целите на политиката. Внатрешната контрола вклучува управување со ризик, усогласеност со внатрешните процедури и упатства, но и со надворешното законодавство и регулативи, периодични и ад-хок извештаи на раководството, проверки за напредокот и ревидирање на плановите, вршење ревизии, евалуации и мониторинг[7].

[7] IT Governance in Public Sector: A Top Priority – WGITA IntoIT Issue 25, August 2007.

Управување со ризик[8]

Управувањето со ИТ ризици треба да биде интегрален дел од стратегијата за управување со ризици на субјектот. Управувањето со ризици вклучува одредување ризици во врска со постојните апликации и ИТ инфраструктура и континуирано управување, вклучувајќи годишна/периодична проверка и ажурирање на ризиците од страна на раководството, како и мониторинг на стратегии за намалување на ризиците.

Механизам за усогласување

Субјектите треба да имаат механизам за усогласување кој обезбедува следење на сите политики и придружни постапки. Механизмот за поддршка на усогласеноста може да вклучува и група за осигурување на квалитет, лица одговорни за безбедност, автоматизирани алатки итн. Раководството треба да ги разгледува извештаите за неусогласеност, а сериозните и повторливи проблеми за неусогласеност/ непочитување мора брзо да се решаваат. Раководството може да се справи со ова прашање со помош на обуки, измена на процедури, или преку интензивирање на постапките за казнување во зависност од природата на неусогласеноста/непочитувањето (нарушување на безбедноста, отсуство од задолжителна обука, итн.).
Независното осигурување во форма на внатрешна или надворешна ревизија (или проверка) може да обезбеди навремени повратни информации за усогласеноста на ИТ со политики, стандарди, постапки и генералните цели на субјектот. Овие ревизии/проверки мора да се извршуваат на непристрасен и објективен начин со цел раководителите да добијат правилно оценување на ИТ системот кој се ревидира.

Одлуки за инвестиции (развој и набавка на решенија)

ИТ управувањето треба да обезбеди решенија за нови системи или надградба на системите, доколку се оцени дека е тоа потребно. Решенијата можат да се реализираат од страна на ИТ секторот со развивање (градење) на нов софтвер или системи или со набавка на истите од добавувачи со цел ефективна заштеда на трошоци. За успешно спроведување на истото, добрата пракса најчесто вклучува дисциплиниран пристап со кој барањата се утврдуваат, анализираат, подредуваат по важност и одобруваат, се врши анализа на трошоци за конкурентските решенија, по што се избира оптимално решение (на пример, она што одржува рамнотежа меѓу трошоците и ризиците).

ИТ операции

ИТ операциите се всушност секојдневното функционирање на ИТ инфраструктурата за поддршка на тековниот процес. Правилно управување со ИТ

[8]За подетален опис види Поглавје за ИТ безбедност.

операциите овозможува откривање тесни грла и планирање на очекувани промени на капацитетите (дополнителен хардвер или мрежни ресурси), проверка и оценка на изведбата за да се осигури остварување на договорените потреби. ИТ секторот нуди поддршка и информации (help desk) за справување со инциденти на корисниците на ИТ ресурсите.

ИТ ресурси

Се препорачува, по пат на редовни проценки, раководството да обезбеди распределување на доволно ресурси за ИТ со цел остварување на потребите на субјектот согласно договорените приоритети и буџетски ограничувања. Исто така, политиките, праксата и ИТ одлуките треба да го почитуваат човечкиот аспект земајќи ги во предвид тековните и идните потреби на учесниците во процесот. Раководство треба редовно да врши проценка дали ИТ ресурсите се користат и им се дава приоритет согласно бараните цели.

Ризици за субјектот на ревизија

Ревизорите треба да ги познаваат и оценат различните компоненти на структурата на ИТ управувањето за да утврдат дали ИТ одлуките, насоките, ресурсите, раководството и надзорот ги поддржуваат стратешките цели. За спроведување на оценувањето, ревизорот треба да ги знае клучните компоненти на ИТ управувањето. Ревизорот треба да е свесен за ризиците од несоодветноста на било која компонента на ИТ управувањето во субјектот.
Секој субјект се соочува со различни предизвици во зависност од опкружувањето, политичките, географските, економските и социјалните проблеми.
Последици кои може да се појават поради несоодветно ИТ управување, а кои треба да ги има во предвид ревизорот се:

ИТ системи кои се неефективни, неефикасни или тешки за користење: Системите на јавната администрација чија цел е да му служат на општеството, на дејноста или да ја подобрат функционалноста на државните органи, најчесто се сложени решенија со широк опсег. Истите треба правилно да се дизајнираат, да се креираат согласно реалните потреби, квалитетно да се координираат и ефикасно да се спроведат. Слабото ИТ управување на државно ниво и на ниво на субјект може да биде прва пречка за располагање со квалитетни ИТ системи.
ИТ функција без насоки која не е во служба на деловните потреби: Значајните ИТ инвестиции кои не се стратешки усогласени со целите и ресурсите на субјектот резултираат со мала или никаква вредност за работењето. Поради таква стратешка неусогласеност дури и квалитетна ИТ инвестиција не може да придонесе за ефективно и ефикасно постигнување на целите на субјектот. Со цел да се постигне усогласеност со ИТ инвестициите и постигнување на поставените цели потребно е да се инволвираат сите корисници и други засегнати страни.
Ограничувања на развојот на субјектот: Несоодветното или недоволно ИТ планирање може да доведе до ограничен развој поради недостиг на ИТ ресурси или

неефикасната употреба на постојните ресурси. За да се ублажи овој ризик, потребно е периодично ажурирање на ИТ стратегијата со што ќе се дефинираат ресурсите и плановите за задоволување на идните потреби на работењето.

Неефективно управување со ресурси: Со цел да се постигнат оптимални резултати со минимален трошок, субјектот мора ефикасно и ефективно да управува со своите ИТ ресурси. Обезбедувањето доволно технички, хардверски, софтверски и човечки ресурси за давање ИТ услуги е клучен фактор за добивање вредност од инвестициите во ИТ.

Несоодветно донесување одлуки: недоволната информираност на раководството од страна на стручните служби може да резултира со несоодветно одлучување. Тоа, пак, може да влијае на правилно исполнувањето на обврските на субјектот, како и на извршувањето на мандатот. ИТ секторот или друга организациска структура помага во донесувањето одлуки кои влијаат врз работата на субјектот.

Неуспешни проекти: Многу субјекти не успеваат да ја согледаат значајноста на ИТ управувањето. Тие започнуваат ИТ проекти без детално да ги разберат барања за проектот и како тој проект е поврзан со целите. На овој начин ИТ проектите се осудени на неуспех. Истото се случува и во набавките и/или воведувањето на апликации кои не ги исполнуваат минималните стандарди за ИТ безбедност и ИТ инфраструктура. Ваквите проекти бараат дополнителен напор за одржување и администрирање на нестандардни системи и апликации. Еден начин за намалување на ризикот од неуспешни проекти е дефиниран развој и животен век на систем (System Development and Life Cycle) и негово користење при развој и/или набавка.

Зависност од трети страни (добавувачи): Во случај да нема соодветни постапки за процесот на набавка и ангажирање надворешни соработници, субјектот може да се доведе до ситуација да зависи само од еден добавувач или изведувач. Прво, се работи за високо-ризично опкружување бидејќи доколку добавувачот престане да работи или не ја испорача договорената услуга, субјектот ќе се најде во тешка состојба. Постојат и други проблеми, на пример спорови околу интелектуална сопственост, системи и бази на податоци. Субјектите кои редовно склучуваат договори со добавувачи или ангажираат надворешни соработници треба да воспостават политика за ангажирање надворешни соработници или набавка со која ќе се дефинира што може, а што не може да се врши надвор од субјектот.

Недостиг на транспарентност и отчетност: Отчетноста и транспарентноста се два важни елементи на доброто управување. Транспарентноста е моќно средство чија доследна примена може да помогне во борбата против корупцијата, да го помогне управувањето и да ја унапреди отчетноста[9]. Оттука, во отсуство на соодветни организациски структури, стратегии, процедури и надзорни контроли, субјектот нема да успее да работи отчетно и транспарентно.

Извештаи за неусогласеност со закони и регулативи: Ревизорот бара уверување дека субјектите работат согласно законската регулатива и добрата практика за управување во нивното опкружување. Исто така, од причина што информатичката технологија придонесува за непречени деловни процеси меѓу субјектите, се јавува потреба од вклучување значајни ИТ барања во договорите во контекст на

[9] ISSAI 20, Concepts of accountability and transparency, p.4.

обезбедување приватност, доверливост, интелектуална сопственост и безбедност (Cobit 5 Рамка, Принцип 5 и Усогласеност). Политиките за ИТ безбедност, ангажирање надворешни соработници, човечки ресурси, итн. мора да ја вклучат потребната законска регулатива.

Изложеност на ризици за информацискатa безбедност: Голем број ризици за информацискатa безбедност се јавуваат поради отсуство на соодветни структури, процеси и политики, како на пример: проневера на средства, неовластено обелоденување на информации, неовластен пристап и подложност на логички и физички напади, прекин и недостапност на информации, злоупотреба на информации, неусогласеност со законите и регулативите за лични податоци, неможност да се обнови системот по катастрофа. ИТ безбедносната политика треба да ги дефинира организациските средства (податоци, опрема, деловни процеси) за кои е потребна заштита и линк до соодветните процедури, алатки и контрола на физички пристап.

Ревизорска програма

Ревизорската програма од Прилог 2 е почетна точка за вршење оценка на воспоставените контроли за намалување и за управување со ризиците во ИТ управувањето.

Важно е да се запомни дека прашањата во врска со ИТ управувањето се дел од целокупната оценка на ревизорите за општото контролно опкружување во субјектот.

2.6.2. Ревизија на развој и набавка на ИТ решение

Со цел остварување на стратешките цели на субјектот на ревизија, се нудат различни ИТ решенија. Потребите за ИТ решенија се утврдуваат во соодветни документи на субјектот, како на пример стратешки документи, акциони планови, годишни програми итн.

ИТ решенијата може да се развијат од страна на субјектот, да се набават, да се добијат со ангажирање на надворешни соработници или комбинација од сите наведени. Изборот на ИТ решението треба да ги има во предвид расположливите ресурси (човечки и материјални) во институцијата, управувањето со ризиците и целосно задоволување на корисничките барања и потреби. Досегашните искуства покажуваат дека постојните ИТ решенија во јавниот сектор во РМ најчесто се набавени како готови решенија. Ваквиот тренд е присутен и во светски рамки бидејќи овој начин овозможува поголема економичност, а ваквите решенија се широко достапни. Сепак ризиците поврзани со ваквото решение се реално присутни од аспект дека набавеното решение може во целост да не ги задоволува барањата и потребите на корисниците.

При набавката на ИТ решение потребно е субјектот целосно да ги познава своите потреби и барања. Поради тоа процесот на одредување на барањата треба да ги вклучи сите засегнати страни кои се дел од процесите на субјектот меѓу кои и крајните корисници и вработените кои ќе бидат задолжени за одржување и

поддршка на истиот. ИТ одделот треба да биде вклучен во одредување на барањата, во останатите фази на имплементација на ИТ решението и во комуникацијата со добавувачот.
Дефинирањето барања е само прв чекор во процесот на набавка. Набавката вклучува и управување со многу други области како што се: ризици, управување со програми, тестирање, надзор врз добавувачи за време на набавката и подоцна, доколку тие го поддржуваат или администрираат системот, како и вклучување на внатрешни обуки и/или проблеми со воведувањето. Субјектите би требало да обезбедат и осигурување на квалитет и тестирање како гарант за квалитет на ваквите решенија.
Најчесто, решенијата се создаваат или набавуваат од страна на проектен тим.

Клучни елементи при развој и набавка на ИТ решение

При развој или набавка на ИТ решенијата субјектот на ревизија потребно е да ги има во предвид следните клучни елементи:

1. **Одредување и управување со барањата/потребите**.

При развој или набавка на ИТ решенијата субјектот на ревизија неопходно е своите потреби и барања за соодветно решение да ги документира. При одредување на барањата значајно е да постои план, постапка или процедура за начинот на прибирање, анализа и подредување на барањата согласно дефинирани критериуми, независно дали се работи за набавка на ново ИТ решение или надградба на постојното. Барањата треба да бидат јасни и концизни.
Вака документираните барања овозможуваат нивно подредување по приоритет согласно критериумите (на пр. ресурси, трошоци, сложеност и ризици, рок за извршување итн.) и поделба по фази доколку не можат да се спроведат целосно. Со анализа и распоред на барањата по приоритет, субјектот е во можност да донесе одлука за избор на оптимално решение. При донесување на одлуката за избор на ИТ решение се почитува законската регулатива во областа на јавните набавки чие ревидирање е детално опишано во Прирачникот за ревизија на регуларност.

2. **Избор на добавувач за ИТ решение**

Изборот на добавувач за ИТ решение е процес на документирање на барањата на субјектот како и собирање дополнителни материјали кои ќе му помогнат на добавувачот да го испорача ИТ решението. Ова вклучува утврдување на конкретни барања за ИТ решението, негово објавување, прибирање понуди и правење избор на добавувачи согласно Законот за јавни набавки.
Процесот на селекција треба да биде транспарентен, објективен и заснован врз соодветни критериуми за системот или услугите кои се набавуваат.
Во процесот на дефинирање на барањата и селекција на добиените предлози, потребно е да бидат инволвирани лица кои имаат познавање и компетенција од соодветната област.

3. Следење и контрола на реализацијата на ИТ решението

По изборот на ИТ решение следната фаза е следење и контрола на сите чекори од планот за реализација и имплементација на решението. Планот за реализација на проектот се состои од дефинирање на ресурсите и нивно распределување по компоненти, временска рамка на реализација на поодделните компоненти и вклучување на засегнатите страни за клучни активности. Планот на проектот служи како основа за управување со активностите.
Контролата на проектот подразбира надзор и периодично известување за преземање корективни мерки кога реализацијата на проектот не се одвива во согласност со планот. Периодичните кратки известувања до повисокото раководство овозможуваат следење на статусот на проектот и начинот на кој се управува со ризиците. Начинот на следење и контрола при развојот на ИТ решението треба да е опишан во упатства и процедури за тестирање на имплементацијата на решението. Добра пракса за следење на спроведувањето на ИТ решението е постоење на проектен тим составен од проектен менаџер, службеник за ризик, персонал за поддршка на осигурување на квалитет и управувањето со конфигурации, персонал од групата за тестирање доколку не се дел од групата за осигурување на квалитет и други.

4. Осигурување на квалитет и тестирање

Осигурувањето на квалитет овозможува увид на проектниот тим и раководството во квалитетот и функционалноста на привремените и финалните ИТ решенија. За таа цел, вработените вклучени во осигурувањето на квалитет периодично ги оценуваат решенијата за да се осигури дека тие ги задоволуваат стандардите за квалитет предвидени во проектната документација од страна на субјектот и дека вработените ги следат потребните процеси за развој на производите. Субјектите треба да потврдат дали развиеното или набавеното решение ги задоволува барањата и утврдените критериуми (на пр. помалку од одреден број некритични грешки) и дали поминал тестови во кои се вклучени корисници и други учесници. Вработените за осигурување на квалитет треба исто така да потврдат дали се следи усвоената и договорената развојна методологија и дали се врши потребниот надзор. На пример, тие проверуваат дали се спроведени проверки (формални или неформални) и дали се испратени неопходните извештаи за статус до соодветните засегнати страни и раководството. Понатаму, преку вработените за осигурување на квалитет, повисокото раководство може да добива информации за тоа дали проектниот тим ги следи внатрешните политики и постапки за набавка или развој.

5. Управување со конфигурација

Управувањето со конфигурација е постапка која треба да осигури дека имплементацијата на новото ИТ решение нема да го наруши интегритетот на

документите, софтверот и другите материјали кои се работни производи од системот. Лицата задолжени за управување со конфигурација вршат одобрување и/или авторизација на ИТ решението за употреба во продукциска средина. Ова одобрување се прави по извршено корисничко тестирање и останатите тестови потребни за да се потврди дека другите системи функционираат исто како и пред да се инсталира новиот систем или софтвер.

Ризици за субјектот на ревизија

Кога субјектот развива сопствено ИТ решение, постојат голем број ризици или предизвици со кои се соочува, со цел да осигури успешност на решението. Ваквите ризици се поврзани со вештини во изработка на софтвер, искуство за тестирање и управување со проекти, разумни трошоци и проценки на придобивки, но и можност да се надгледува и следи статусот на проектот.

Понатаму, прибирањето и одобрувањето на барањата за соодветен софтвер треба да ги вклучи корисниците, а ревизорите ќе утврдат дали корисниците биле консултирани при дефинирањето на барањата и дали персоналот вклучен во осигурување квалитет објективно го вреднува квалитетот на системот кој се развива. Како и кај набавувањето, потребно е раководството периодично да биде известувано за статусот на проектот, како би се презеле потребните корективни мерки.

Кога вршат ревизија кај субјектот кој набавил системско решение, основната цел на ревизорите е да одредат дали субјектот има редовна комуникација со добавувачот, дали добива периодични извештаи за статусот на системот и дали презема корективни мерки. За таа цел, договорот мора да ги наведе клучните одредници за време на развојот на системското решение онаму каде има формална проверка и извештаи за статусот на решението кои му даваат информации на субјектот за ресурсите, временскиот распоред и постигнувањата. Ревизорот треба да се увери дали раководството на субјектот или назначениот персонал добива, проверува и презема соодветни корективни мерки во однос на извештаите за статусот и договорените активности.

Ревизорска програма

Прашањата подложни на ревизија за оценување на стратегиите за развој на системот од страна на субјектот или негова набавка можат да се најдат во ревизорската програма во Прилог 3 – Ревизорска програма за ревизија на развој и набавка на ИТ решение.

2.6.3. Ревизија на ИТ операции

Под поимот ИТ операции се подразбираат секојдневните задачи при работа и поддршка на информациските системи во еден субјект (сервери и нивно одржување, изнаоѓање неопходно место за складирање, поддршка итн.). Операциите се мерат и

управуваат со помош на клучни индикатори за изведба на ИТ операции (КИИ) кои претставуваат параметри со кои може да се мери оперативната ефективност. Овие индикатори или нивни еквиваленти вообичаено се документираат и периодично се проверуваат. Повеќето субјекти ги документираат КИИ со еден вид договор меѓу нив и ИТ организацијата која го реализира решението.
Во меѓународната пракса ова е познато како Договор за услуга.

Клучни елементи на ИТ операциите

Слика 3.1 Области на ИТ операции

Некои од областите или елементите на ИТ операциите кои ревизорот ќе треба да ги разгледа со цел да одреди дали субјектот на ревизија ефективно управува со ИТ операциите се: дизајн и испорака на услуги, капацитет и управување со услуги, постапки за справување со инциденти со цел осигурување на континуитет на операциите и практики при управувањето со промени. Овие и слични области се дефинирани во една од најширо прифатените рамки за одредување, планирање, испорака и поддршка на ИТ услуги во компаниите ITIL[10].

Со цел да се одреди дали субјектот на ревизија ефективно ги испорачува документираните услуги, ревизорот треба да го користи договорот во кој се наведени посебни параметри за различни услуги.

Управување со континуитет на ИТ услуги

Целта на управувањето со континуитет е да ги одржува соодветните барања за постојан деловен континуитет. ИТ организацијата ова го постигнува со определување на временски период за повторно воспоставување на одделните ИТ компоненти кои ги поддржуваат деловните процеси врз основа на договорените барања и критериуми. Понатаму, управувањето со континуитет подразбира периодична проверка и ажурирање на времето на повторно воспоставување како би се обезбедила согласност со Плановите за деловен континуитет (ПДК) и деловните

[10] ITIL, http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

приоритети. (Оваа област е подетално објаснета во делот Ревизија на план за деловен континуитет и план за обновување по катастрофа)

Управување со безбедноста на информациите

Управувањето со безбедноста на информациите е поврзано со управување со ризици поврзани со нивната безбедност, преземање соодветни мерки и осигурување дека информациите се достапни, корисни, комплетни кога се потребни. Управувањето треба да осигури дека само овластени корисници имаат пристап до информациите и дека истите се заштитени кога се пренесуваат од една на друга локација и се доверливи кога пристигнуваат. Оваа област е подетално објаснета во делот Ревизија на информациска безбедност.

Управување со капацитети

Управувањето со капацитети подразбира управување со различни услуги кои го поддржуваат работењето на начин кој ги следи деловните потреби на субјектот на ревизија или корисниците. Оптимизирањето на капацитетот на мрежниот проток, достапност на ресурси, оптимизацијата и зголемувањето на простор за складирање се составни делови на управувањето со капацитет. Со цел да се управува со капацитетот, ИТ организацијата која го реализира решението ги оценува тековните состојби и потреби како би презела активности, со кои на корисниците им се овозможува дополнителен капацитет. Покрај тоа, за една ИТ организација која испорачува услуги на одреден субјект, управувањето со капацитет би било ефективно доколку се ангажира соодветно квалификуван/обучен ИТ кадар, доволно ресурси и алатки со што би се овозможило соодветен надзор над мрежата и услуги за поддршка, а ангажираниот персонал би бил активно вклучен во справувањето со тесни грла, истовремено одговарајќи на деловните потреби.

Управување со проблеми и инциденти

Управувањето со инциденти се однесува на системите и практиките кои се користат за одредување дали инцидентите или грешките се навремено забележани, анализирани и решени. Управувањето со проблеми е насочено кон решавање прашања преку испитување и детална анализа на поголемите или повторливи инциденти за да се открие причината на нивното настанување. Штом еден проблем е откриен и е направена детална анализа на причината за проблемот, тој станува позната грешка или неефикасност, па може да се развие решение за негово надминување и спречување понатамошна појава на слични инциденти. Потребно е да се воведе механизам за откривање и документирање на условите кои може да доведат до идентификација на инциденти. Единицата за ИТ операции треба да поседува документирани постапки за откривање и документирање инцидентни, како Прирачник или компјутеризиран дневник во состав на специјализиран ИТ софтвер. Како примери на инциденти може да се наведат неовластени пристапи или упади на корисници (безбедносни), падови на мрежата (оперативни), слаба

функционалност на софтверот (испорака на услуги) или недостиг на вештини кај крајните корисници (обука).

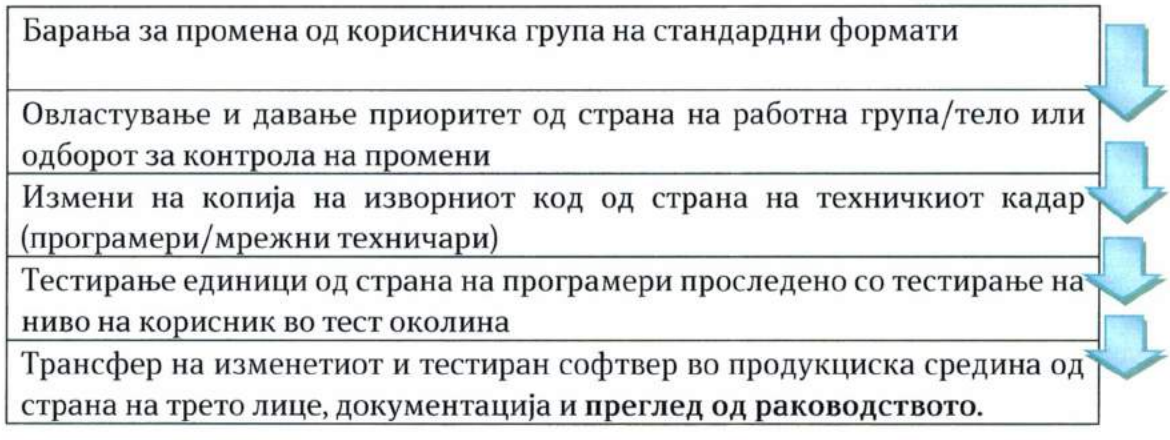
Управување со промени

Управувањето со промени е процес кој служи за управување и контролирање промени кај средствата како што се софтверот, хардверот и придружната документација. Контролата на промените е потребна со цел да осигури дека сите промени во системската конфигурација се овластени, тестирани, документирани и контролирани како би можело системите да продолжат да ги поддржуваат деловните операции на планираниот начин, но и за да се утврди дека постои соодветна трага од промените.

Неовластена или случајна промена може да доведе до сериозен ризик и финансиски последици за субјектот на ревизија. Субјектите следат дефинирана постапка за управување со промени која бара одобрение од раководните структури пред да се спроведе во опкружувањето. Процесот на управување со промени треба да осигури дека промените се евидентирани, оценети, одобрени, со утврден приоритет, планирани, тестирани, имплементирани, документирани и ревидирани во согласност со документираните и одобрени постапки за управување со промени.

Промените можат да бидат иницирани со промена на деловната средина, измена на деловниот модел, внатрешно организациски потреби или како резултат од анализата на одреден инцидент.

Во сликата подолу се објаснети чекорите при управување со промени.



Слика 3.2 Чекори во управувањето со промени

Трошокот за промената, влијанието врз ИТ системот и деловните цели, ефектите од неспроведување и понатамошните барања за ресурси се значајни фактори при одобрување и давање приоритет на промените.

Промените во итни случаи не можат да ги следат вообичаените постапки за контрола на промени и мора да се спроведат со минимално одложување. Времето за воведување и тестирање на промената е намалено. Ова создава повисок ризик за грешки и програмски пропусти.

Онаму каде постојат постапки за итни промени, ревизорот проверува дали тие се оправдани и вклучуваат некаква форма на контрола. Ова вклучува и одобрување итна промена од овластено лице, соодветен назив на верзијата и контрола заедно со ревизорска трага (употреба на автоматизирани апликации за контролирање промени), ретроспективно одобрение од раководството на субјектот за промени/сопственикот на системот, ретроспективно тестирање и ажурирана документација.

Утврдување на ниво на услуги

Договор во кој е утврдено ниво на услуги ги документира параметрите кои ИТ организацијата, која го спроведува решението, ги користи за да испорача услуги до субјектот. За параметрите најчесто согласност даваат субјектите на ревизија и ИТ организацијата која го спроведува решението. Ревизорот ги користи параметрите од договорот за да оцени дали ИТ организацијата го постигнува нивото на услуги и дали субјектите на ревизија се задоволни или се преземаат соодветни мерки во случај да се јават отстапки од договорените параметри за ниво на услуги. Договорот меѓу другото ги содржи и клучни индикатори за изведба (КИИ) за ИТ услугите. Разгледувањето на КИИ ќе му помогнат на ревизорот да постави прашања за:

- Дали системите функционираат согласно документираните договори;
- Дали се воспоставени механизми за откривање пропусти во работата, за посочување на откриени пропусти и следење на имплементацијата на преземените корективни мерки како резултат на оценувањето на изведбата на субјектот;
- Одредување контролни точки кај субјектот на ревизија со што се одредува природата, периодот и обемот на тестирањето.

На пример, параметри за КИИ и соодветните дефиниции и цели за управување со промени се дадени подолу:

Процес	Цел (Критичен фактор за успех)	Клучни индикатори за изведба (КИИ)	Хронологија на мерки
Управување со промени	Намалување инциденти предизвикани со неовластени промени	Процентно намалување на бројот на инциденти кои произлегуваат од неовластен пристап	Се следи преку управување со инциденти, управување со промени и се дава месечен извештај.

Ризици за субјектот на ревизија

Најважен доказ за ревизорот е Договорот со кое е утврдено нивото на услуги. Во него се содржани параметрите, критериумите за изведба и барањата според кои се оценува ИТ организацијата која го спроведува ИТ решението. Доколку во овој договор ги нема или не е формално прегледан и одобрен од деловните сопственици,

постои ризик дека ИТ ресурсите во субјектот нема да се искористат на најефективен или најефикасен начин. При ревизија на ИТ операции, потребно е ревизорот да го добие договорот во кој е дефинирана општата цел и техничките параметри за ИТ операциите, како и периодични извештаи од ИТ организацијата кои го мерат и известуваат за статусот на индикаторите, како и преглед на раководството и секакви активности или насоки на ИТ организацијата во кои се забележуваат значајни отстапувања од параметрите.

Во областа на управувањето со промени, ревизорот треба да провери дали постојат процедури за контрола на промени кои обезбедуваат интегритет на системот како и гаранција дека само одобрените и тестирани апликации се воведени во оперативното опкружување.
Ревизорот треба да го согледа начинот на кој субјектот управува со капацитетите (уред за складирање на податоци, централна единица за обработка, мрежни ресурси итн.), проактивност на субјектот при одговор на барањата на корисниците, како и начинот на управување со инциденти и други безбедносни прашања за да не се компромитираат деловните функции.

Ревизорска програма
Ревизорската програма за овој дел може да се најде во Прилог 4 – Ревизорска програма за ревизија на ИТ операции.

2.6.4. Ревизија на ангажирање надворешни соработници

За функционирање на веќе воспоставен деловен процес или за доделување нова деловна функција субјектот може да ангажира надворешни соработници. Начинот на нивно ангажирање треба да се регулира со договор.
Субјектот треба да има политика или визија за кои аспекти или деловни функции (најчесто ИТ, но може и други) ќе ангажира надворешни соработници, а кои функции ќе ги извршува интерно. Во зависност од ризичноста на услугата односно нејзиното значење за деловниот процес за кој се ангажираат надворешни соработници, субјектот може да избере да врши подетални или поопшти формални контроли врз таквата услуга. Субјектот може да одлучи дали за сите или само за некои од операциите ќе ангажира надворешни соработници бидејќи ваквата практика нуди одредени придобивки меѓу кои:

Флексибилност при вработувањето

Ангажирањето надворешни соработници дозволува операциите кои имаат времен или периодичен карактер да поттикнат прилив на дополнителни ресурси кога субјектот има потреба, а со завршувањето на времените операции истите да престане да ги користи.

Развој на кадар

Доколку ИТ решението/процесот бара вештини кои субјектот не ги поседува, субјектот наместо да ги обучува вработените, може да ангажира надворешни соработници со што би се заштедило на трошоци за обуки и време. Оттука, сметајќи на физичката локација и техничката експертиза на добавувачот, субјектот може да ги ангажира своите вработени да соработуваат со кадарот на добавувачот на одреден период, со што вработените би добиле практична обука.

Намалување на трошоците

Ангажирањето надворешни соработници во одредени случаи ги намалува трошоците за работна сила кај субјектот. Субјектот кој нема расположив кадар квалификуван да ја заврши задачата, може да ангажира надворешни соработници со цел да ги намали трошоците. Пример за ова би бил ангажирање на надворешни соработници за софтверска задача која бара специјализирана обука.

Експерти на повик

Со ангажирањето надворешни соработници субјектот е во можност да има експерти на повик кои се подготвени да помогнат за тековни или идни проблеми. Со помош на експертите, субјектот може брзо да одговори на променетите деловни потреби (нова мисија или воведување дополнителни функции).

Примери на ангажирање надворешни соработници

Според документот на **ISACA за ангажирање надворешни соработници**[11], субјектите можат да ангажираат надворешни соработници за различни области од работата и ИТ инфраструктурата, како што се:

- Оперативна инфраструктура која може да содржи центар за податоци и придружни процеси;
- Обработка на апликации во субјектот од страна на испорачател на услуги;
- Развој на системи или одржување апликации;
- Инсталација, одржување и управување со персоналните компјутери и придружни мрежи.

Последниот новитет во ангажирањето надворешни соработници е кај т.н. работење во „облак" (cloud computing)[12]. Во овој случај, субјектот ангажира надворешни соработници за обработка на податоци на компјутери во сопственост на добавувачот. Добавувачот е домаќин на опремата, додека субјектите сè уште имаат

[11] Outsourced IT Environments Audit /Assurance Program, 2009.

[12] Види Водич и прирачник на работната група за ИТ ревизија за ревизија на обработка во облак

контрола врз апликацијата и податоците. Ангажирањето надворешни соработници може исто така да опфати и користење на компјутерите на добавувачот за складирање, правење резервни копии на податоци и овозможување онлајн пристап до податоците на субјектот. Субјектот мора да има стабилен и брз пристап до интернет доколку сака вработените или корисниците да имаат постојан пристап до податоците, па дури и до апликацијата која ги обработува податоците. Во работната средина, податоците или апликациите се достапни и на мобилните платформи (лаптопи со Wi-Fi или мобилни картички, паметни телефони и таблети).
Примери на работење во „облак" се апликации засновани врз електронска пошта и заеднички деловни апликации до кои се пристапува преку интернет пребарувач, наместо преку локален компјутер.

Клучни елементи на ангажирањето надворешни соработници

Политика за ангажирање надворешни соработници

Потребно е субјектот да има политика во која е дефинирано за кои функции може да се ангажираат надворешни соработници, а кои функции мора да се извршуваат внатре во субјектот. Најчесто, субјектите ангажираат надворешни соработници за рутинските ИТ операции, одржување, па дури и хардверските платформи за персонални компјутери. Досиејата на вработените и политиката на управување со човечки ресурси се извршуваат во субјектот бидејќи истите бараат директен надзор и се предмет на повеќе закони и стандарди за приватност и безбедност, па не би било економично и ефективно за истите да се ангажираат надворешни соработници.
Ревизорот треба да започне со разгледување на постапките и политиката за ангажирање надворешни соработници кај субјектот. Поголемите субјекти кои за значаен дел од деловните операции ангажираат надворешни соработници неопходно е да имаат одобрена политика за ангажирање надворешни соработници во која јасно се образложени процесите на спречување на незаконски дејствија и други неправилности во постапката. Помалите субјекти може и да немаат формална политика, но треба да следат ефикасни и транспарентни процеси на спречување на незаконски дејствија и други неправилности во постапката.

Спречување на незаконски дејствија и други неправилности во постапката – избор на надворешни соработници

Спречување на незаконски дејствија и други неправилности во постапката е процес на документирање на барањата на системот и прибирање други дополнителни материјали со чија помош добавувачот ќе го изгради системот. Овде станува збор и за создавање на понуда, добивање на предлози и правење избор на добавувачи. Процесот на селекција треба да биде транспарентен, објективен и заснован врз критериуми соодветни за системот или услугите кои се набавуваат согласно Законот за јавни набавки.

Управување со добавувачи / договори

Управувањето со добавувачи е клучен елемент на ангажирањето надворешни соработници со цел да се осигури дека дадените услуги ги задоволуваат очекувањата на субјектот. Субјектот треба да има воспоставени постапки за периодично следење на статусот на ИТ решението/процесите, квалитетот на услугата, потврдено тестирање на создадените производи пред да се пуштат во оперативно опкружување итн.
Ревизорот треба да процени дали субјектот ги одредил своите критериуми за ангажирање надворешни соработници пред да го избере добавувачот (посебните барања и оперативни параметри се содржани во договорот), дали субјектот следи дали добавувачот ги исполнува критериумите наведени во договорот (со периодични извештаи за статусот на реализација), дали субјектот презел мерки кога добавувачот не постапил согласно договорените параметри (корективни мерки или парични казни).

Утврдување на ниво на услуги

Договор меѓу субјектот и добавувачот ангажиран како надворешен соработник и претставува клучна алатка за следење и контрола на услугите реализирани од добавувачот.
Договорот ги дефинира услугите кои добавувачот треба да ги изврши, како и техничките параметри за тие услуги.
Области кои ги покрива договорот се следните:

- Видот на услуги кои добавувачот ќе ги изврши;
- Распределување одговорности меѓу субјектот и добавувачот;
- Услугите кои ќе се оценуваат, периодот на оценување, времетраење, локација и периоди за известување (стапка на дефекти, време на одговор, работно време на делот за поддршка итн.);
- Време на воведување нова функционалност, изготвување на верзии на функционалност;
- Вид на потребна документација за апликациите креирана од добавувачот;
- Локација на која ќе се извршуваат услугите;
- Фреквенција на правење на резервна копија, параметри за поврат на податоци;
- Прекин/Комплетирање и методи и начини за испорака на податоци;
- Клаузули за мотивација и казни.

Договорот мора да ги содржи елементите кои се значајни за субјектот. Ревизорот треба да го побара договорот и да процени дали извештаите на добавувачот во поглед на параметрите ги задоволуваат барањата содржани во договорот и дали субјектот ги презел потребните корективни мерки во однос на пропустите.

Остварување на придобивки

Субјектите најчесто ангажираат надворешни соработници со цел намалување на трошоците. Ова се практикува кога трошоците за испорака на услугите се пониски кај добавувачот отколку да се ангажира внатрешна инфраструктура или работна сила. Постојат и други придобивки кои не се директно мерливи од типот на проширување на инфраструктурата на добавувачот доколку настане брз раст на нивото на услуги или користење на нивната експертиза во посебни случаи. По можност, субјектот треба периодично да прави пресметки и анализи со цел да одреди дали планираната заштеда е постигната. Ова служи како една од значајните точки за одредување дали да се продолжи или прекине со ангажирање надворешни соработници.

Безбедност

При ангажирање надворешни соработници за бази на податоци и нивно администрирање, субјектот мора да процени дали добавувачите имаат доволно ефективни безбедносни практики и дали можат да ги задоволат безбедносните барања кај субјектот, согласно стандардите за безбедност, како на пример ISO 27000. Додека повеќето субјекти сметаат дека безбедноста кај добавувачите е импресивна (често ги надминува внатрешните практики), ризикот од безбедносни прекршоци или заштитата на интелектуална сопственост инхерентно се зголемува заради фактот дека податоците се дадени на надворешни соработници. Посебно внимание мора да се обрне и на проблемите со приватноста. Останатите безбедносни проблеми се однесуваат на можна злоупотреба или обелоденување чувствителни податоци, неовластен пристап до податоци и апликации и план за обновување по катастрофи. Иако ваквите прашања не претставуваат пречки за ангажирање надворешни соработници, критериумите мора да се документираат.

Ризици за субјектот на ревизија

1. **Зачувување на деловното знаење и сопственост на деловниот процес**

При ангажирање на надворешни соработници постои инхерентен ризик од загуба на деловно знаење кое им припаѓа на креаторите на ИТ решението. Доколку од некаква причина креаторите на ИТ решението односно добавувачот не се во можност да ја испорачаат услугата односно решението, субјектите на ревизија мора да бидат подготвени да го реализираат решението согласно законската регулатива. Понатаму, од причина што развивањето на апликацијата/ИТ решението се случува надвор од субјектот, постои ризик субјектот да се одрече или да ја изгуби сопственоста врз деловниот процес, за кој испорачателот на услуги може да тврди дека е негова интелектуална сопственост. Субјектите треба да го земат предвид ова прашање при потпишувањето договор и да се погрижат да ја имаат целосната документација од процесот на развој на системот и од неговото дизајнирање. Со тоа субјектот би можел да ги смени и добавувачите на услуги, доколку се јави потреба.

2. Неиспорака од страна на добавувачот

Понекогаш, добавувачот може да не успее да испорача одреден производ навремено или истиот не може да се прифати поради нефункционалност. Доколку процесот на спречување на незаконски дејствија и други неправилности во постапката не е правилно спроведен, постои висока веројатност дека системот или услугите кои се набавуваат нема да ги исполнат очекувањата на корисникот, ќе бидат со понизок стандард, ќе чинат повеќе, ќе бараат значителни ресурси за одржување и оперирање или можат да бидат со толку слаб квалитет што ќе мора во блиска иднина да се заменат. Некои од причините на неиспорака од страна на добавувачот се лош договор, несоодветни критериуми за избор на добавувачи, нејасни одредници и/или неповолни пазарни услови.
Субјектот би требало да има резервни планови во таков случај. При одлуката за ангажирање надворешни соработници, субјектите треба да ги оценат последиците од неуспех на добавувачот (т.е. дали неуспехот има сериозни последици по функционирањето на субјектот?). Достапноста на детална документација за дизајн на системот и негов развој би му помогнало на субјектот да овозможи деловен континуитет со избор на друг добавувач на услуги или самостојно.

3. Неконтролирани промени во обемот на работа

Сите договори за ангажирање надворешни соработници содржат стандарди и барања. Доколку реалната работа отстапува од договорената вредност, субјектот ја плаќа разликата. При имплементација на проекти постои можност од менување вредност на договорот во текот на развојниот циклус, но разликата мора да биде оправдана согласно развојниот процес на проектот а во рамките на законската регулатива.

4. Надворешни ризици

Доколку се ангажира меѓународен добавувач на услуги како надворешен соработник, особено во работење во т.н. „облак" (cloud computing), постојат ризици кои се однесуваат на странските регулативи за складирање на информации и нивен трансфер кој може да ограничи што може да се складира и како може да се обработи, ризици поврзани со користење на податоци без знаење на субјектот на ревизија доколку така налагаат законите на странската земја, не пропорционалност кај стандардите за приватност и безбедност, а поради различната правна регулатива, споровите не можат целосно да се избегнат.

Ревизорска програма

Ревизорската програма може да се најде во Прилог 5 – Ревизорска програма за ревизија на ангажирање надворешни соработници.

2.6.5. Ревизија на план за деловен континуитет и план за обновување по катастрофа

Соодветното функционирање и достапноста на компјутерските системи имаат многу важна улога во остварувањето на мисијата на секој субјект, особено во многу значајни активности како што се пресметка и наплата на даноци и царини, пресметка и исплата на плати и придонеси, пензии, социјални надоместоци, статистички податоци за наталитет, морталитет, криминал, болести итн. Всушност, многу од овие активности не би можеле да се извршат точно и ефективно без компјутерски техники.

Прекин на електрична енергија, природни катастрофи и злонамерни штети можат да имаат разорно влијание врз информациските системи. Потребно е доста време за субјектот да почне ефективно да работи доколку не постои функционален план за деловен континуитет (Business continuity plan - BCP, ПДК) и план за обновување по катастрофи (Disaster recovery plan – DRP, ПОК).

Поимите план за деловен континуитет и план за обновување по катастрофи се користат како синоними, но всушност се работи за два различни поими. И двата плана имаат голема важност од причина што овозможуваат по настаната катастрофа да се обезбеди остварување на мисијата на субјектот и задржување на способноста да се процесираат, повлечат и заштитат информациите во случај на прекин или настаната штета поради привремено или трајно губење на компјутерските функции.

Планот за деловен континуитет е процес кој субјектот го користи за планирање и тестирање на обновените деловни процеси по одреден прекин. Со овој план се опишува начинот на кој субјектот ќе продолжи да функционира при појава на природни или други катастрофи. Планот содржи политики, процедури и практики со чија помош субјектот ги обновува и враќа во употреба рачните и автоматски процеси критични за мисијата по настанување на катастрофа или криза. Покрај постапките кои треба да се следат при прекин, некои планови содржат активности за обновување по катастрофа, одговори во итен случај, обновување на корисници и управување со кризи.

Планот за обновување по катастрофа без разлика дали е посебен документ или е составен дел на планот за деловен континуитет треба да ги дефинира потребните ресурси, активности, задачи и податоци за управување со процесот на обновување во случај на прекин на работата. Овој план треба да му помогне на субјектот при повратна погодените работни процеси преку приказ на чекорите кои треба да бидат преземени за обновување. Поточно кажано планот за обновување по катастрофа се користи за неопходни детални подготовки и планови со цел намалување на штети од настанатите прекини. Во однос на ИТ, планот се однесува на обновување критични технолошки средства меѓу кои и системи, апликации, податоци, бази на податоци, уреди за складирање на податоци и други мрежни ресурси.

Обемот на Планот за континуитет во работењето и планот за обновување по катастрофа и деталните мерки значително варираат во различни субјекти. Субјектите кои имаат големи ИТ сектори со современи информациски системи и сложени комуникациски мрежи имаат потреба од сеопфатни, најнови планови за континуитет и опоравување кои вклучуваат и спремни паралелни капацитети како алтернатива. Од друга страна пак, помалите субјекти без одделни сектори, кои користат само десктоп компјутери и едноставни софтверски пакети, имаат едноставни планови.

Плановите за континуитет во работењето и обновување по катастрофа треба да бидат документирани, повремено да се тестираат и доколку е неопходно да се ажурираат. За да се утврди дали овие планови ќе функционираат како што треба, истите треба периодично да се тестираат со симулирање на ситуација на катастрофа.

Потребата и значењето на овие планови е поголема, доколку одговорноста е на неколку клучни вработени во ИТ секторот. Доколку овие клучни луѓе си заминат, истото ќе има неповолно влијание врз способноста на субјектот да продолжи со работењето во разумен временски период.

Од ревизорот се бара да ги оцени плановите на субјектот за деловен континуитет како и планот за обновување по катастрофа.

Кога ќе врши оценка на соодветноста на планот за континуитет во работењето и обновување по катастрофа, ревизорот треба:

- Да изврши оценка на плановите за континуитет во работењето и обновување по катастрофа за да ја утврди нивната адекватност, преку прегледување на плановите и на нивната усогласеност со организациските стандарди и/или законската регулатива.
- Да потврди дека плановите за континуитет во работењето и обновување по катастрофа се ефективни и обезбедуваат брзо продолжување на работењето, преку прегледување на извршените тестирања (доколку има) од страна на ИТ секторот и крајните корисници.
- Да изврши оценување на просториите за складирање кои се наоѓаат надвор од субјектот, преку прегледување на просториите, на она што се наоѓа во нив и на контролите за безбедност и контроли на опкружување. Може да се утврди и дали резервните копии кои биле направени порано биле некогаш тестирани за враќање на податоци од страна на субјектот на ревизија.
- Да изврши оценување на способноста на ИТ лицата и на останатите вработени кои се корисници на системот да реагираат ефективно во итни ситуации, преку прегледување на процедурите за итни случаи, на обуката за вработените и на резултатите од процедурите.

Ефективното планирање на деловен континуитет содржи неколку фази заеднички за сите информациски системи. Општи чекори во процесот се:

- Политика и план и субјектот за деловен континуитет;
- Воспоставување на функцијата за деловен континуитет;

- Проценка на деловно влијание (ПДВ) и управување со ризици;
- Превентивни контроли меѓу кои и контроли на опкружување;
- План за обновување по катастрофи;
- Тестирање на планот за деловен континуитет;
- Безбедност во текот на спроведувањето на ПДК / ПОК;
- Правење резервни копии и обновување по катастрофи за услугите за кои се ангажирани надворешни соработници.

Секој од наведените елементи ќе ги објасниме во продолжение.

Политика, план и организација на деловниот континуитет

Ефективното планирање на континуитет започнува со воведување политика за деловен континуитет. Раководниот тим за деловен континуитет кој ги претставува сите соодветни деловни функции игра важна улога во успехот на планот за деловен континуитет. Политиката на планот за деловен континуитет ги дефинира севкупните цели за континуитет и ја утврдува рамката и обврските за планирање континуитет.

Воспоставување функција за деловен континуитет

За да биде успешен, раководниот тим за деловен континуитет мора да биде организиран да ги претставува неопходните деловни функции. Раководството и другите вработени мора да ја поддржуваат програмата за континуитет и да учествуваат во процесот на развој на политиката. Улогите и задачите на тимот треба да бидат јасно одредени и дефинирани.

Проценка на деловно влијание и управување со ризици

- *Проценка на критичноста и чувствителноста на компјутеризираните операции и одредување ресурси за поддршка*

Во секој субјект, континуитетот на одредени процеси е значаен, а од друга страна не е исплатливо да се одржува истото ниво на континуитет за сите процеси. Од таа причина, важно е да се одреди кои се најкритични процеси и кои ресурси се потребни за обновување и поддршка. Тоа се врши со помош на проценка на ризици, одредување можни закани и нивното влијание врз организациските, информациски и придружни ресурси како што се податоците, апликацискиот софтвер и операциите. Проценката на ризици и влијанија треба да ги покрие сите функционални области. Потребно е да се донесе одлука за преостанатите ризици каде влијанието од можните закани е минимално или контролните системи да се приспособени за навремено откривање на таквите случаи.

- *Идентификација и давање приоритет на критични податоци и операции*

Критичноста и чувствителноста на различните податоци и операции се одредува и утврдува врз основа на безбедносните категоризации и севкупната проценка на

ризици за операциите на субјектот. Таквата проценка треба да послужи како основа за безбедносен план. Меѓу факторите кои треба да се земат предвид спаѓаат важноста и чувствителноста на податоците и другите средства, како и трошокот за ненавремено складирање податоци и операции. На пример, еднодневен прекин на главните системи за наплата на данок или загуба на поврзани податоци може значително да го забави или прекине приемот на приходи, да ја намали контролата врз приходите и да ја намали довербата на јавноста. Од друга страна, системот кој врши надзор врз обуките на вработените може да не функционира неколку месеци, а тоа да нема сериозни последици.

Генерално земено, критичните податоци и операции треба да се идентификуваат и рангираат од страна на персоналот вклучен во програмските операции. Важно е за таквите одлуки да се добие согласност и од раководството.

Листата со приоритети во однос на критичните информациски ресурси и операции периодично се проверува за да се утврди дали тековните состојби имаат некакво влијание. Проверките се вршат секогаш кога ќе настанат значајни промени во мисијата и операции или во локацијата или дизајнот на системите поддржани од овие операции.

▫ *Одредување ресурси за поддршка на критични операции*

Веднаш по одредувањето критични податоци и операции, треба да се одредат и минималните ресурси потребни за нивна поддршка, истовремено со анализа на нивните улоги. Ресурси кои треба да се земат предвид се: компјутерски ресурси меѓу кои хардвер, софтвер и податочни датотеки; мрежи со делови од типот на рутери и „заштитни ѕидови"(firewall), набавки кои вклучуваат залихи на хартија и изготвени формулари, телекомуникациски услуги и други ресурси неопходни за операцијата како што се луѓе, канцелариски капацитети и материјали, но и некомпјутерзирани досиеја.

Од причина што суштинските ресурси се управуваат од страна на повеќе групи во субјектот, важно е персоналот за информациска безбедносна поддршка да работи заедно за да се одредат потребните ресурси за критичните операции.

▫ *Утврдување приоритети за итна обработка*

Во врска со одредувањето и рангирањето критични функции, субјектот треба да развие план за враќање критични операции во функција. Планот треба јасно да го одреди редоследот по кој различните аспекти на обработка ќе се враќаат во функција, кој е одговорен и каква опрема за поддршка или други ресурси ќе бидат потребни. Внимателно развиен план за обнова на обработката ќе им помогне на вработените веднаш да започнат со процесот на реконструирање и најефикасно искористување на ограничените компјутерски ресурси во итен случај. И корисниците на системот и персоналот за поддршка на информациска безбедност треба да учествуваат во одредувањето приоритети во случај на итна обработка.

▫ *Спречување и намалување на потенцијални штети и прекини*

Постојат повеќе чекори кои субјектот може да ги направи за спречување или намалување на штетата врз автоматските операции кои настануваат при неочекувани прекини. Истите може да се категоризираат на следниот начин:

- рутинско копирање или правење резервни копии на податочни датотеки, компјутерски програми и критични документи кои се складираат на друга локација, и/или организирање далечни капацитети за резервни копии кои ќе можат да се користат доколку вообичаените капацитети на субјектот се оштетат и се вон употреба;
- утврдување капацитет за реконструкција на информациски системи со цел обновување и реконструирање на информацискиот систем во неговата првобитна состојба по одреден прекин или пад;
- воведување контроли на опкружување како противпожарни системи или резервно напојување;
- осигурување дека персоналот и другите системски корисници ги разбираат своите одговорности за време на итен случај;
- ефективно одржување хардвер, управување со проблеми и управување со промени.

▫ *Имплементација на процедури за заштита на податоци и програми*

Рутинското копирање папки на датотеки со податоци и софтвер и складирањето на овие досиеја на безбедна, далечна локација се најисплатливите активности кои субјектот може да ги преземе со цел ублажување прекини во услугите. Иако опремата може брзо да се замени, трошокот може да биде висок, а реконструирањето компјутеризирани папки на датотеки со податоци и заменувањето софтвер е прескапо и предолго трае. Некои податочни датотеки не секогаш може да се реконструираат. Освен директниот трошок при реконструирање досиеја и набавување софтвер, придружните прекини во услугите може исто така да доведат до големи финансиски загуби.

▫ *Обуки*

Вработените треба да се обучуваат и да бидат свесни за своите обврски за спречување, ублажување и реагирање во итни случаи. На пример, вработениот за поддршка на информацискатa безбедност треба повремено да се обучува за постапки кои следат во случај на пожар, поплава и други инциденти, како и за нивните обврски за започнување и водење на алтернативна локација за обработка на податоци. Понатаму, доколку надворешните корисници се критични за операциите на субјектот, тие треба да бидат информирани за чекорите кои треба да ги преземат во итен случај.

▫ *Планови за одржување хардвер, управување со проблеми и управување со промени*

Неочекувани промени во услугите може да настанат од дефект во хардверската опрема или од менување опрема без претходно соодветно да се информираат корисниците. За да се спречат такви случаи, потребна е ефективна програма за

одржување, управување со проблеми и управување со промени во хардверската опрема.

Контроли на опкружување

Контролите на опкружувањето спречуваат или ублажуваат потенцијални штети на капацитетите или прекини на услугите. Следуваат неколку примери на контроли на опкружувањето:

- системи на апарати за гаснење пожар и противпожарни апарати;
- аларми за пожар;
- детектори за чад;
- детектори за вода;
- осветлување во итни случаи;
- дополнителни системи за воздушно ладење;
- резервно напојување;
- вентили за исклучување и постапки за сите водоводни линии во зградата кои можат да ги доведат во опасност капацитетите за обработка;
- капацитети за обработка изградени од материјали отпорни на пожар и дизајнирани со цел да го намалат ширењето оган;
- политики кои забрануваат јадење, пиење и пушење во рамките на компјутерските капацитети.

Контролите на опкружувањето може да ги намалат загубите од прекини настанати поради пожари или да ги спречат инцидентите со рано откривање потенцијални проблеми како што се истекување вода или чад за навремено да се реагира. Резервни напојувања со енергија може да му помогнат на субјектот во случај на краток енергетски прекин или пак, да овозможат време за заштита на податоците и соодветно исклучување на системот.

План за обновување од катастрофи

Планот за обновување по катастрофи се развива за повратна критични апликации што вклучуваат ангажмани за алтернативни капацитети за обработка во случај на делумно оштетување или неможност за пристап до вообичаените капацитети. Политиките и постапките на организациско ниво го дефинираат процесот на планирање, обнова на системот и потребната документација. Понатаму, организацискиот поширок план треба да ги одреди критичните системи, апликации и останати подредени или придружни планови. Од особена важност е ваквите планови да бидат јасно документирани, пренесени до засегнатиот персонал и ажурирани со цел да се однесуваат на тековните операции.

▫ *Документација за ажуриран план за обнова*

Плановите за обнова на системот треба да бидат документирани, одобрени од субјектот и одделот за информациска безбедност и пренесени до вработените за кои се однесуваат. Планот треба да ги одразува ризиците и оперативните приоритети кои субјектот ги идентификувал. Трошоците за планирање на обнова не треба да ги

надминуваат трошоците поврзани со ризиците кои планот треба да ги намали. Планот треба да биде доволно детален и документиран за неговиот успех да не зависи од знаењето или експертизата на едно или две лица.
Потребни се повеќе копии од планот, а некои треба да се наоѓаат и на подалечни локации со цел да не се оштетат од истите настани кои ја оневозможиле работата на примарните капацитети за обработка на податоци.

▫ *Организирање алтернативни локации*
Во зависност од потребниот степен на континуитет на услуги, изборот на алтернативни локации или капацитети ќе варира од опремена локација подготвена за итна заштита на податоци т.н. „hot site" до неопремена локација за која ќе треба одредено време да се стави во функција т.н. „cold site". Понатаму, различните услуги можат претходно да се договараат со добавувачите. Тоа подразбира правење договори со испорачатели на компјутерски хардвер и телекомуникациски услуги како и испорачатели на деловни формулари и останати канцелариски материјали.

Тестирање

▫ *Периодично тестирање на планот за континуитет*
Тестирањето планови за континуитет е неопходно со цел да се одреди дали тие ќе функционираат како што е испланирано во итни случаи. Тестовите ги откриваат најслабите точки на плановите, како на пр. капацитетите за заштита кои не можат соодветно да ги обноват критичните операции. Со процесот на тестирање, таквите планови значително се подобруваат.
Застапеноста на тестирањето планови за континуитет ќе зависи од критичноста на операциите. Најопшто земено, плановите за континуитет за покритични функции треба целосно да се тестираат еднаш на една или две години, секогаш кога ќе се направат видливи измени на планот или во случај на поголема промена на клучен персонал. Од голема важност е раководството да ги процени ризиците од проблемите кај планот за континуитет и да се развие и документира политика за зачестеноста и обемот на тестирањето.

▫ *Ажурирање планови за континуитет врз основа на резултати од тестовите*
Резултатите од тестот за континуитет даваат мерливи податоци за остварливоста на планот за континуитет. Тие треба да му се пренесат на високото раководство со цел да се одреди потребата од измени и дополнително тестирање, како и негово информирање за ризиците од продолжувањето со работа без несоодветен план за континуитет.

Безбедност

Безбедноста на ресурсите и операциите треба да биде составен дел од деловниот план за континуитет бидејќи критичните податоци, апликацискиот софтвер, операциите и ресурсите можат лесно да се изложат на опасност за време на прекин или при активност за управување со деловниот континуитет. На пример, за време на

правењето резервни копии на податоци, недостиг на безбедност може да доведе до создавање дупликати и загуба на важни податоци. Истовремено, можно е податоците за кои се прават резервни копии да бидат изложени на опасност и во текот на самиот процес.

Правење резервни копии и обнова на податоци за услугите за кои се ангажирани надворешни соработници

Многу субјекти ангажираат надворешни соработници за сите или дел од активностите кај одреден вршител на услуги. Поаѓајќи од фактот дека секојдневните операции и контроли ќе ги извршува испорачателот на услуги, субјектот ќе мора да се осигури дека планот за деловен континуитет и обновување по катастрофи е вметнат во договорот. Субјектот ќе треба да врши надзор врз степенот на подготвеност на испорачателот на услуги за деловниот континуитет и обновувањето по катастрофи. Ова подразбира и негова безбедносна подготвеност. Субјектот ќе мора да се осигури дека испорачателот на услуги го обезбедува потребното ниво на доверливост на податоците во апликацискиот софтвер кој го одржува. Сопственоста на деловниот процес ја задржува субјектот. Субјектот треба да има и план за континуитет со цел да обезбеди континуитет во случај на статусни промени на испорачателот на услуги.

Ризици за субјектот предмет на ревизија

Критични услуги или производи се оние кои мора да бидат испорачани за да обезбедат опстанок, спречат предизвикување загуби и да ги исполнат законските и другите обврски на субјектот. BCP/DRP или ПДК/ПОК е процес на проактивно планирање кој овозможува деловните процеси и ИТ инфраструктурата на субјектот да ги поддржат потребите на мисијата по одреден пад или прекин на работата на системот. Субјектите кои извршуваат повеќе критични потреби на граѓаните (исплати на граѓаните, овозможување здравствена заштита, образование, одбрана и други услуги), и доколку овие услуги се во прекин подолг период, тоа може да доведе до финансиски и други загуби. Ревизорите треба да се погрижат сите субјекти да имаат постапка за ПДК/ПОК со цел истите да продолжат со работа и да бидат во служба на граѓаните.

При оценувањето дали процедурите на ПДК/ПОК можат да ги гарантираат и заштитат веродостојноста и континуитетот на ИТ инфраструктурата и деловниот процес, постојат неколку ревизорски ризици на кои ревизорите треба да посветат внимание при оценувањето ефективност на деловниот континуитет и планот за обновување од катастрофи. Тие треба да содржат развој на планови за обновување од катастрофи и деловен континуитет за да се покријат сите критични функционални области. Доколку обновувањето од катастрофи на критична функционална област е загрозено, истото ќе му се случи и на деловниот континуитет. Доколку улогите и обврските не се јасни и разбрани од надлежните лица, дури и солиден план за континуитет може да стане неефективен.

Постапката за проценка на деловното влијание, превентивните контроли и контролите на опкружувањето, документацијата, тестирањето на планот за континуитет и обучувањето соодветен персонал го потпомагаат ефективното спроведување на планот за деловен континуитет. Недоволната безбедност при спроведување план за деловен континуитет и план за обновување по катастрофи претставува ризик од губење податоци, загуба на време и други трошоци кои произлегуваат од неефективното обновување од катастрофата.
Услугите за кои се ангажирани надворешни соработници исто така преставуваат ризична област каде ПДК/ПОК не се под целосна контрола на субјектот. Постои ризик за безбедноста на податоците, неовластено работење и загуба на податоци кои треба да се земат предвид.

Ревизорска програма

Ревизорската програма може да се најде во Прилог 6 – Ревизорска програма за ревизија на план за деловен континуитет и план за обновување по катастрофа.

2.6.6. Ревизија на информациска безбедност

Информацискатa безбедност се дефинира како способност на системот да ги заштити информациите и ресурсите во однос на доверливоста и интегритетот. Таа се однесува на заштита на информациите и информациските системи од неовластен пристап или промена на информации, без разлика дали тие се складирани, во обработка или пренос, како и непрекината услуга на овластените корисници. Безбедноста на информациите ги вклучува и мерките потребни за откривање, документирање и следење на ваквите закани. Безбедноста на информациите му овозможува на субјектот да ја заштити инфраструктурата на информацискиот систем од неовластени корисници и се состои од Информацискатa безбедност и комуникациска безбедност.
Основен аспект на ИТ управувањето од кој зависат сите други работни процеси е безбедноста на информациите во делот на **достапноста, доверливоста** и **интегритетот**. Информацискатa безбедност е од огромна важност за институцијата и претставува чувар на информациските средства на субјектот. За тоа е потребна политика за безбедноста на податоците со која ќе се заштитат податоците на субјектот, која истовремено може да му овозможи на субјектот да ги оствари деловните цели и со прифатливо ниво на ризик во текот на работењето. Обезбедувањето на информации на овластените лица е исто толку значајно колку и заштитата на информациите од оние кои не треба да ги добијат. Безбедноста мора да овозможи функционалност и да ги поддржи деловните цели, а не да функционира сама за себе.

Потреба од информациска безбедност

Информацискатa безбедност станува сè поважна за државните институции заради поврзаноста на јавните и приватните ИТ мрежи како и споделувањето

информациски ресурси со што се зголемува сложеноста на контролата на пристап и зачувување на доверливоста, интегритетот и достапноста на податоците.
Информациските системи се комплексни состави на технологија, процеси и луѓе кои соработуваат со цел приспособување на обработката, складирањето и пренесувањето информации за да се поддржи мисијата на субјектот и неговото функционирање. Оттука, секој субјект задолжително треба да има политика за информациска безбедност.
Целта на политиката за безбедност на информацискиот систем е да се заштитат информациите од субјектот преку доведување на ризикот од загуба на доверливост, интегритет и достапност на информациите до едно прифатливо ниво. Доколку субјектот нема гаранција за безбедност на информациите, ќе мора да се соочи со ризици и потенцијални закани за функционирањето на субјектот, постигнувањето на целокупните цели, а последици ќе претрпи и авторитетот на субјектот.
Со порастот на можностите, сложеноста и улогата на информатичките технологии, информациската безбедност станува сè поважна област во ИТ ревизиите. Таа е критичен фактор на активностите на субјектот бидејќи недостатокот на информациска безбедност може да предизвика сериозни последици како што е непочитување на законски и подзаконски акти, влошување на реномето на субјектот, финансиски штети, намалување на продуктивноста и ранливост на системот со подложност на неовластен пристап.
Ваквите штети може да се предизвикани од нарушување на безбедноста, неовластени надворешни конекции или изложеност на информациите со обелоденување чувствителни информации.

Креирање свесност за безбедност на информациите

Показател за успешноста на програмите за информациската безбедност во субјектот е создавањето свесност во однос на безбедносните прашања. За таа цел, кај големите субјекти потребен е модел на информациска безбедност кој ги содржи следниве елементи:

- **Развивање на свеста за безбедноста:** Се состои од активности и образовни сесии со цел подигање на свеста за информациската безбедност меѓу вработените.
- **Поголема посветеност на раководството:** Посветеноста на раководството е незаменлив атрибут во формирањето свест за информациска безбедност која се гледа не само преку приготвување формална документација за политиките за безбедност на информациите, туку и преку активна вклученост и присуство во субјектот. Не поддржување на политиката за информациска безбедност од раководството го обесхрабрува чувството за обврска или одговорност за политиката кај другите вработени.
- **Координација со формирање меѓу-секторски функционални тимови:** Бидејќи информациската безбедност содржи многу аспекти кои бараат координација, потребно е формирање на меѓу-секторски функционални тимови со што се поттикнува комуникацијата, соработката, се намалува изолираноста на одделни сектори и се избегнува дуплирање на активностите.

Воведувањето свесност за информациска безбедност се карактеризира со неколку особини:

- **Усогласување на информацискатa безбедност и целите на субјектот,** бидејќи на тој начин се овозможуваат и поддржуваат истите. Политиката за информациска безбедност се усогласува со субјектот и бара контролите за безбедност на информациите да бидат практични и да придонесуваат за реално и мерливо намалување на ризикот.
- **Проценката на ризици** треба да се надополни во примената на информацискатa безбедност за да се одреди потребната форма на контрола. Заобиколувањето на проценка на ризиците може да предизвика заканите по безбедноста на информациските системи да резултираат во оштетени инфраструктури кои биле заштитени или во некои случаи и постоела непотребно голема заштитеност. Примената на проценка на ризиците му помага на раководството да избере соодветни контроли за ефикасно ублажување на ризиците.
  Проценката на ризици подразбира одредување и анализа на:
  - сите средства и процеси поврзани со системот;
  - потенцијални закани кои можат да ја загрозат доверливоста, интегритетот достапноста на системот;
  - слабите точки на системот и придружните закани;
  - можни влијанија и ризици од активноста на заканите;
  - стандарди за заштита со цел ублажување ризици;
  - избор на соодветни безбедносни мерки и анализа на поврзаност со ризиците.
- **Рамнотежа меѓу раководството, вработените, процесите и технологијата:** Ефективната информациска безбедност бара поддршка од раководството, обучени вработени, ефикасни процеси и избор на соодветна технологија. Сите овие елементи взаемно делуваат, ги поддржуваат и влијаат врз другите елементи на сложени начини и од тој аспект неопходно е да се постигне рамнотежа меѓу нив. Доколку само еден елемент недостасува, безбедноста на информациите се намалува.

Клучни елементи на информацискатa безбедност

За успешно спроведување на безбедноста на информацискиот систем, постојат неколку клучни елементи кои мора да се земат предвид:

- **Доверливост** - подразбира овластени ограничувања за пристап и обелоденување информации, вклучувајќи средства за заштита на лична приватност и информации. Доверливоста се однесува за прашања од областа на приватноста кои мора да бидат пропишани. За одржување на доверливоста, системот мора да се погрижи секое лице да го задржи правото да контролира кои информации за него се собираат, како се користат, кој ги користи, кој ги одржува и за каква цел се користат.
- **Интегритет** - се однесува на заштита од несоодветни измени или оштетувања на информациите, што подразбира осигурување на неотповикливост и автентичност на информациите. Автентичноста подразбира оригиналност и овозможување потврда и доверба во валидноста на преносот, пораките или

креаторот на пораката. Со цел да се потврди интегритетот на информациите, потребен е механизам за автентичност кој ќе потврди дали корисниците се оние лица што се претставуваат дека се. Постапката овозможува информациите кои се создаваат или пренесуваат да ги задоволат стандардите за неотповикливост. Неотповикливост подразбира сигурност дека испраќачот на информациите има доказ за испорака, а примачот има доказ за идентитетот на испраќачот, па ниту еден од нив подоцна не може да негира дека ја обработил информацијата.

- **Достапност** - овозможува сите информациски системи вклучувајќи го и хардверот, комуникациските мрежи, софтверските апликации и податоците кои тие ги содржат да им бидат достапни на корисниците во секое време со цел вршење на работните активности. Сепак, следењето на безбедносниот принцип за употреба на овие ресурси бара воспоставување на политика за контрола на пристап. Целта на контролата на пристап е да се обезбеди дека корисниците пристапуваат само до ресурсите и услугите за кои се овластени и нема да бидат одбиени за услугите за кои се авторизирани за кои се овластени.

Информацискатa безбедност во субјектот покрива **дванаесет области** и тоа:

1. Проценка на ризици

Проценката на ризици е процес на одредување, анализирање и проценување на ризиците во безбедноста на ИТ инфраструктурата. Се работи за процес на проценување безбедносни ризици од внатрешни и надворешни закани по субјектот, неговите средства и вработените. Подетално оваа област е разработена во Прилог 7 - Ревизорска програма за ревизија на информациска безбедност во делот за Проценка на ризици.

2. Политика за безбедност

Политиката за безбедност на субјектот претставува збир на подзаконски акти, политики и процедури кои го утврдуваат начинот на кој субјектот раководи, ги заштитува и испорачува ресурсите со цел да ги постигне одредените безбедносни цели. Овие подзаконски акти, политики и процедури треба да одредат критериуми за надлежноста на вработените и да ги посочат условите под кои на нив им е дозволено да ги вршат работите согласно своите овластувања. За да бидат применливи, овие акти мора да им овозможат на вработените да одредат дали со нивните активности ја почитуваат безбедносната политика.
Подетално оваа област е разработена во Прилог 7 - Ревизорска програма за ревизија на информациска безбедност во делот за Политика за информациска безбедност.

3. Организација на ИТ безбедноста

Организацијата на ИТ безбедноста подразбира воведување безбедносна политика во субјектот. Оваа задача може да му се додели на еден сектор или лице кое работи во ИТ одделот за стекнување соодветни алатки и спроведување на активности за

воведување на безбедносната политика. Друга задача е да се спроведуваат почетна и тековна обука на вработените и оние кои работат на безбедносни инциденти. Постои потреба и од правилна заштита на податоците на субјектот кон кои се пристапува или податоци кои се пренесуваат до надворешни субјекти. Ревизорот треба да процени дали субјектот е способен да ги исполни утврдените ИТ критериуми. Подетално оваа област е разработена во Прилог 7 - Ревизорска програма за ревизија на информациска безбедност во делот за Организација за ИТ безбедноста.

4. Управување со комуникации и операции

Субјектот треба да води сметка за процесите и постапките кои ги користи во работните активности со кои се овозможува точна обработка на податоци. Тука спаѓа документирање на постапки за управување со медиуми и податоци, постапки во итни случаи, безбедно мрежно најавување и постапки за правење резервни копии на податоци. Подетално оваа област е разработена Прилог 7 - Ревизорска програма за ревизија на информациска безбедност во делот за Управување со комуникации и операции.

5. Управување со средства

Пошироко земено, управувањето со средствата се однесува на секој систем каде основните средства на субјектот постојано се надгледуваат и одржуваат. Тоа подразбира постојан процес на ракување, одржување, ажурирање и располагање со средствата на ефективен начин.
Во информатичката технологија, управувањето со средства подразбира одржување точна листа на ИТ опрема, познавање кои лиценци за која опрема се однесуваат, како и одржување и заштита на опремата. Управувањето со ИТ средствата вклучува и управување со софтверот и документацијата за процесите важни за субјектот. Подетално оваа област е разработена во Прилог 7 - Ревизорска програма за ревизија на информациска безбедност во делот за Управување со средства.

6. Безбедност кај човечките ресурси

Вработените кои работат со лични податоци во субјектот треба соодветно да се обучат и запознаат со заштитата на податоците кои им се доверени. Потребно е да се дефинираат и документираат соодветните улоги и обврски кои се доделени на секое работно место и тоа да се усогласи со безбедносната политика на субјектот. Податоците на субјектот мора да се заштитат од неовластен пристап, обелоденување, измени, уништување или попречување. Управувањето со ризиците по безбедноста и приватноста на човечките ресурси е неопходно за време на сите фази на еден работен ангажман во субјектот (при вработување, за време на работниот ангажман и при прекин или промена на работното место).

Потребно е да се воведе политика за подигање на свеста за безбедност која ќе ги потсетува сите вработени за можните ризици и изложувања, како и за нивните обврски како „чувари" на информациите на субјектот.
Безбедноста подразбира и трошоци, а од друга страна никогаш не може да биде совршена или целосна – безбедноста може да ги намали, но не и целосно да ги отстрани ризиците. Поаѓајќи од тоа дека контролите не се совршени, силната физичка безбедност го применува принципот на силна одбрана користејќи правилни комбинации на контроли кои се поклопуваат и надополнуваат. На пример, физичките контроли на пристап до заштитените капацитети имаат за цел да:

- одвраќаат потенцијални натрапници (на пр. знаци на предупредување и оградување со ознаки);
- прават разлика меѓу овластени и неовластени лица (на пр. со употреба на пристапни картички и клучеви);
- одложуваат, отежнуваат или спречуваат натрапнички обиди (на пр. силни ѕидови, катанци и сефови);
- откриваат обиди за влез и снимаат натрапници (на пр. аларми за влез и камери);
- поттикнуваат соодветни одговори за инциденти (на пр. обезбедување и полиција).

Подетално оваа област е разработена во Прилог 7 - Ревизорска програма за ревизија на информациска безбедност во делот за Безбедност на човечки ресурси.

7. Физичка безбедност и безбедност на опкружувањето

Физичката безбедност опишува мерки наменети за забранет физички пристап за неовластени лица во зградата, капацитетот, ресурсите или складираните информации како и упатства за начинот на создавање структури за спречување потенцијално злонамерни активности. Физичката безбедност може да биде едноставна како на пример, заклучена врата или посложена како повеќеслојни бариери, вооружени чувари и поставување стражарници.
Физичката безбедност примарно се однесува на ограничување физички пристап за неовластени лица во контролирани капацитети, но постојат и други сфаќања и ситуации во кои мерките за физичка безбедност се од големо значење (на пример, ограничување пристап во рамките на капацитетот и/или до специфични средства, како и контроли на опкружувањето со цел намалување физички инциденти како пожари и поплави). Подетално оваа област е разработена во Прилог 7 - Ревизорска програма за ревизија на информациска безбедност во делот за Физичка безбедност.

8. Контрола на пристап

Контролата на пристап подразбира вршење контрола врз секој кој има пристап до ресурсите. Не секогаш, ова вклучува овластено лице кое ја врши контролата. Ресурсите може да бидат одредена зграда, група згради, или компјутерски заснован ИТ систем. Без разлика дали е физичка или логичка, контролата на пристап е

секојдневен настан. Контролата на пристап е од најголема важност за обезбедување на важни, доверливи или чувствителни информации и опрема.
Кај државните институции, контролата на пристап е неопходна бидејќи многу државни субјекти обработуваат чувствителни податоци, а барањата за приватност ограничуваат кој може да има пристап до конкретните податоци. Контролата на пристап овозможува само корисниците со одобрение за соодветен процес да имаат пристап до чувствителните податоци. Подетално оваа област е разработена во Прилог 7 - Ревизорска програма за ревизија на информациска безбедност во делот за Контрола на пристап.

9. Набавка, развој и одржување на ИТ системи

Животниот циклус на развојот на системите (System Development Life Cycle - SDLC) или процесот на софтверски развој во системското инженерство, ИТ системи и софтверско инженерство, е процес на создавање или промена на ИТ системите, како и на моделите и методологиите кои луѓето ги користат за развој на системите. Во софтверското инженерство, концептот на SDLC поддржува повеќе видови методологии за софтверски развој. Овие методологии ја формираат рамката за планирање и контролирање на создавањето ИТ системи или процеси на софтверски развој. Употребата на системот вклучува и промени и подобрувања пред системот да се повлече од употреба. Одржувањето на системот е важен аспект на SDLC. Со менувањето на клучните вработени на други работни места во субјектот, ќе предизвика и промена во системот. Подетално целиот овој процес е опишан во делот Ревизија на развој и набавка на ИТ решение.

10. Управување со инциденти на ИТ безбедност

Во областа на информациската безбедност и информатичка технологија, управувањето со инциденти на ИТ безбедноста подразбира надзор и откривање безбедносни настани на одреден компјутер или компјутерска мрежа и давање соодветни одговори на тие настани. Управувањето со ИТ безбедносни инциденти е посебна форма во целокупниот процес на управување со инциденти . Подетално целиот овој процес е опишан во делот Ревизија на ИТ операции.

11. Управување со деловен континуитет

Планирањето деловен континуитет е процес кој субјектот го користи за планирање и тестирање на враќање на деловни процеси во употреба по одреден прекин. Понатаму, со него се опишува како субјектот ќе продолжи да функционира под отежнати услови (на пример, природна или друга катастрофа). Подетално целиот овој процес е опишан во делот Ревизија на план за деловен континуитет и план за обновување по катастрофа.

12. Усогласеност

Ревизорот треба да ја прегледа и процени усогласеноста со сите внатрешни и надворешни критериуми (закони, подзаконски акти, квалитетот на опкружувањето и информациите, доверливоста и безбедноста).

Ризици за субјектот предмет на ревизија

ИТ безбедносните политики, процедури и нивното спроведување му овозможуваат на субјектот да ја заштити својата ИТ инфраструктура од неовластени корисници. Безбедносната ИТ политика во субјектот ги поставува највисоките барања кои треба да ги следи субјектот и вработените за да се заштитат основните средства. Таа вклучува обука на вработените во однос на безбедноста и гарантира дека тие ги следат утврдените процедури за пристап и контрола на податоци. Понатаму, ИТ политиката се однесува на закони и останата регулатива која субјектот треба да ја почитува. Постојат и пречки со кои таа се соочува во поглед на спроведувањето ефективна безбедност на информации. Без ефективно управување за надминување на таквите ограничувања, ИТ безбедноста е загрозена и тешко може да ги оствари целите на субјектот.

Позначајни ризици со кои се соочуваат повеќето субјекти:

- неовластено обелоденување информации;
- неовластени измени или уништување информации;
- ранливост од ИТ напади;
- уништување на ИТ инфраструктурата;
- неможност за влез или употреба на информации или информациски систем;
- прекини во работата на информацискиот систем;
- украдени податоци или информации.

Најчеста изложеност на ризици на кои треба да им се обрне внимание се следните области:

- **стратегиите** за безбедноста на информациите не се усогласени со ИТ или деловните барања;
- **политиките** не се применуваат подеднакво со различно извршување;
- **несообразност** со внатрешните и надворешните барања;
- безбедноста на информациите не е вклучена во проектите во процесот на одржувањето и развојот;
- **Дизајнираната на системска архитектура** дава неефективни, неефикасни и погрешни решенија за безбедноста на информациите;
- несоодветни мерки за **физичка** безбедност и управување со средствата;
- несоодветна **конфигурација** во примената на хардверскиот систем;
- неефикасна **организација** на процесите за безбедноста на информациите и недефинирана или конфузна структура на ИТ задачи;
- несоодветни решенија за **човечки ресурси;**

- неефективна употреба на **финансиските ресурси** предвидени за безбедноста на информациите, **вредносната** (исплатлива) структура на безбедноста на информациите не е усогласена со деловните потреби или цели;
- не се врши или неефективен **надзор** врз безбедноста на информациите.

Ревизорот започнува со проценување на соодветност на моделите за проценка на ризик и ги зема предвид ревизорските прашања во врска со воведувањето безбедност на информациите. Ревизорска програма во Прилог 7 - Ревизорска програма за ревизија на информациска безбедност ќе му помогне на ревизорот да ги подобри ревизорските прашања, критериумите за оценка, потребните документи и техничката анализа.

2.6.7. Ревизија на апликациски контроли

Апликација е посебен софтвер кој се користи за извршување и поддршка на одделни деловни процеси. Може да содржи рачни и компјутеризирани постапки за иницирање трансакции, обработка на податоци, чување датотеки и подготовка на извештаи. Секој субјект може да има неколку активни апликации – кои може да варираат согласно големината на субјектот - од систем за целиот субјект до кој има пристап секој вработен, до мала апликација до која пристап има само еден вработен. Апликацискиот софтвер може да биде систем за плати, систем за фактурирање, систем за попис или интегриран ERP систем (систем за планирање ресурси во субјектот).

Апликациските контроли претставуваат рачни или автоматизирани постапки кои се спроведуваат на ниво на деловен процес и се применуваат во процесирање на индивидуални апликации[13]. Со проверката на апликациските контроли ревизорот му овозможува на раководството независна проценка на ефикасноста и ефективноста на функционирањето на внатрешните контроли и воспоставените процедури поврзани со автоматизацијата на деловниот процес, како и идентификување на прашањата поврзани со апликациските контроли кои бараат понатамошно внимание.

Ревизијата на апликациите ги проценува внатрешните контроли коишто се однесуваат на влезот, обработката, датотеки и излезот (резултатот) на одредени функции. Сите ревизори кои извршуваат ревизии со примена на системски базиран пристап на административни функции за кои се користи информатичката технологија потребно е да го земат предвид овој аспект на ревизија на информациските системи[14].

Апликациските контроли на сметководствениот систем според видот можат да бидат превентивни или детективни и истите се дизајнирани да обезбедат интегритет на сметководствената евиденција. Според тоа, апликациските контроли се однесуваат на постапки кои се користат за иницирање, евидентирање,

[13] ISSAI 1315, A105

[14] Европски упатства за примена на ревизорските стандарди на INTOSAI 1998, бр. 22. Ревизија на информациони системи, точка 3.7

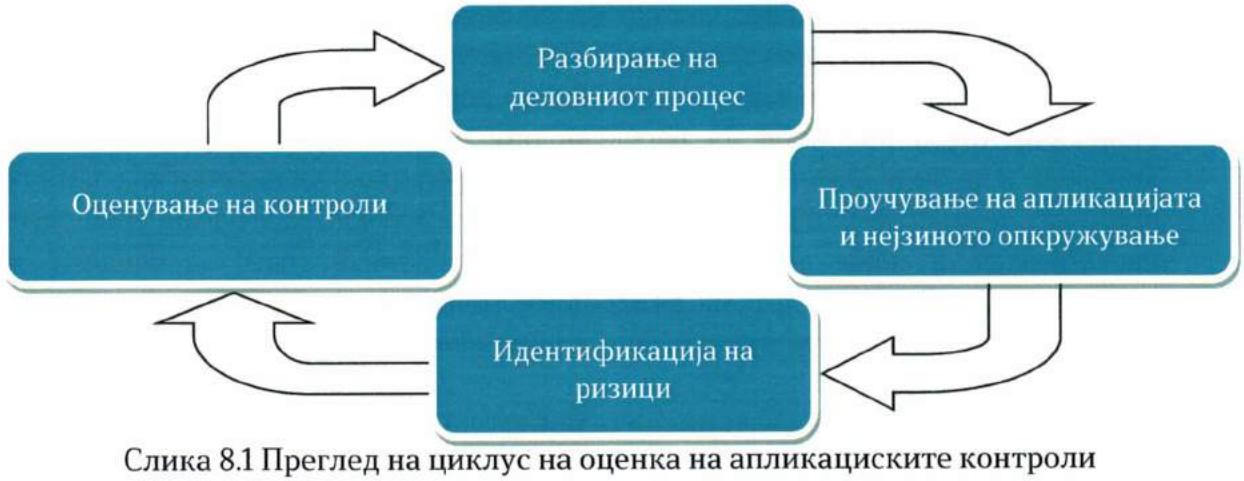
обработување и известување за трансакции или други финансиски податоци. Овие контроли помагаат да се осигури дека трансакциите настанале, дека се овластени и дека се целосно и точно евидентирани и обработени.

Апликациските контроли се поврзани со поединечните трансакции и оттука е очигледно зошто тестирањето на контролите ќе му помогне на ревизорот да ја оцени точноста на одредена функционалност. На пример, тестирањето на контроли во апликацијата за плати може да ги потврди износите за плата на вработените, додека тестирањето на општите ИТ контроли кај субјектот не би овозможило такво ниво на сигурност на платите.

Во зависност од посебните ревизорски цели, оценката на апликациските контроли може да има различни пристапи. Начинот на кој се тестираат контролите може да се разликува од една ревизија до друга. На пример, оценката на апликацијата може да се насочи кон усогласеност со законите и стандардите, па главната активност би била да се утврди дали апликациските контроли соодветно ги адресираат овие аспекти. Од друга гледна точка, оценката на апликацијата може да биде дел од ревизија на успешност и тука би било важно да се оцени како деловните принципи (ефективност, ефикасност, економичност) се вградени во апликацијата. Во текот на анализата на информацискатa безбедност, вниманието може да се насочи кон апликациските контроли одговорни за обезбедување доверливост, интегритет и достапност на податоците.

1. Чекори при оценка на апликациските контроли

Чекорите кои се преземаат при оценка на апликациските контроли може да бидат презентирани во вид на кружен процес на активности. Иако можеби е од интерес оценката на апликациските контроли да се започне со разбирање на деловниот процес, важно е да се напомене дека редоследот на чекорите не е строго определен. Чекорите при оценка на апликациските контроли се наведени подолу и кратко се опишани во текстот што следи.



Слика 8.1 Преглед на циклус на оценка на апликациските контроли

- **Разбирање на деловниот процес:** пред да преминеме на техничкиот аспект на апликацијата, корисно е да добиеме сознанија за деловните процеси кои

апликацијата ги автоматизира, како што се правила, тек, учесници, улоги и соодветни барања за усогласеност. Да се разбере основата на работата е важен чекор со чија помош ќе може да се утврдат апликациските контроли и автоматизираните процеси. Обемот на овој чекор ќе варира согласно ревизорската цел. Најчесто се врши со проучување на оперативните/работни процедури, шемата на текот на процесот во субјектот или друг дополнителен материјал. Исто така, ревизорскиот тим треба да разговара со раководителите, лицата задолжени за ИТ и клучните корисници на апликацијата.

- **Проучување на апликацијата и нејзиното опкружување:** се проучува дизајнот и работењето на апликацијата преку преглед на документацијата (организациски дијаграми, дијаграми за тек на податоци, упатства за користење) или преку интервју со клучните корисници. Клучните функции на софтверот се проучуваат преку набљудување и интеракција со ангажираните вработени во текот на работењето. Преку интервју, се запознаваме со деловниот процес и апликацијата од влезот па се до излезот и усогласувањето, за да се увериме како всушност се одвиваат процесите и да откриеме дали постојат придружни мануелни активности кои може да делуваат како дополнителни контроли. Потребно е да се обезбедат информации од раководството, извршителите и програмерите и да се обезбеди документација за техничката инфраструктура: оперативен систем, мрежна средина, систем за управување со бази на податоци, врски со други внатрешни или надворешни апликации, обработка на влезна серија во реално време/онлајн трансакција. Оваа активност треба да обезбеди доволно показатели за начинот на кој техничката инфраструктура влијае врз апликацијата.
- **Идентификација на ризици:** генерално служи за одредување ризици поврзани со деловната активност/функцијата опслужена од апликацијата (што може да тргне на лошо?) и согледување како софтверот се справува со овие ризици (што го контролира ризикот?). Понекогаш проценката на ризици во деловниот процес може да е веќе достапна (извршена со претходна ревизија, од внатрешна ревизија или од раководството), а ревизорот може да ја користи откако ќе ја оцени довербата во постојната проценка на ризик.
- **Оценување на контролите:** откако ќе се запознае со средината (деловна и техничка) која ја опкружува апликацијата, ревизорот може со поголема сигурност да ги оцени контролите кои се користат за справување со тековните ризици. Ревизорот треба правилно да расудува при оценувањето на апликациските контроли и да биде внимателен при давањето препораки за подобрување. На пр. премногу детално регистрирање на трансакциите може да ги зголеми трошоците на субјектот, а може да не се постигнат потребните траги за следење на трансакциите. Оценувањето на контролите може да се однесува на различни видови на апликациски контроли, кои се опишани во текстот подолу.

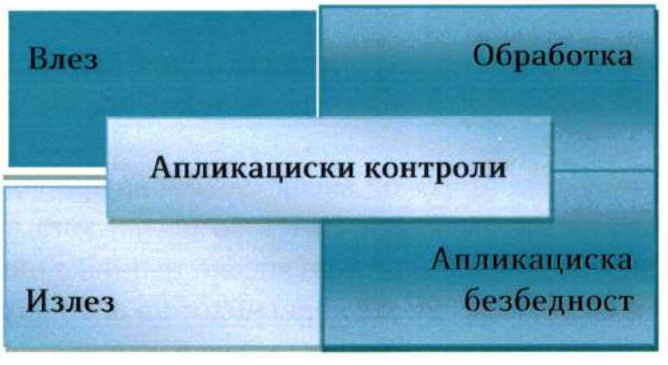
2. Клучни елементи на апликациските контроли

Апликациските контроли се карактеристични за секоја компјутерска апликација. Кога деловните процеси се автоматизираат со помош на апликација, деловните правила се вградуваат во апликацијата во форма на апликациски контроли. Тие се

однесуваат на сегменти од апликациите, а се поврзуваат со трансакциите и постојните податоци. Додека општите ИТ контроли во субјектот ја воспоставуваат целокупната контролна средина за информациските системи, апликациските контроли се вградени во посебни апликации со цел заштита на точноста, интегритетот, веродостојноста и доверливоста на информациите. Тие треба да обезбедат дека иницирањето трансакции е од соодветно овластено лице, дека се обработуваат валидни влезни податоци и дека истите се целосно запишани и дека точно се известува.

Апликациските контроли вклучуваат и мануелни процедури кои функционираат во однос на апликацијата. Овие контроли не се само вградени во посебните апликации, туку и во околината на деловните процеси. На пример, еден службеник за влез на податоци може да побара формуларот за влез на податоци да биде соодветно потпишан (одобрен) пред тие да се внесат во системот. Изборот на комбинација на рачна и автоматизирана контрола е најчесто прашање на разгледување на трошоците и контролите во фазата на создавање на апликацијата.

Апликацијата може да се подели на следните сегменти: внес на податоци (извор на податоци и упис на податоци); обработка на трансакцијата; излез на податоци (обезбедување на резултати) и безбедност (записи, комуникација, чување). Контролите се вградени во секој сегмент на апликацијата.



Слика 8.3 Клучни елементи на апликациските контроли

Иако не е реално да се изготват детални чекори за тестирање и листи за проверка за секоја можна апликацијата, ИТ ревизорот треба да биде запознаен со концептите на контроли заеднички за скоро сите апликации, кои може да бидат надградени во однос на поспецификни ревизорски чекори за тестирање на апликацијата предмет на ревизија.

Најчестите контролни елементи се сликовито прикажани во табелата подолу:

Контроли на влез	• Внес на податоци/ проверка на полиња (на пр. потврда на валиден датум); • Управување со изворни документи (постапки за нивна подготовка и чување); • Постапки за справување со грешки (пораки за грешки, привремени датотеки); • Правила за овластување за внес на податоци (на пр. поделба на должности).

Контроли на обработка	• Мапирање на деловните правила; • Проверување на интегритетот и целосноста на податоците, извештај за неусогласени состојби; • Автоматизирани пресметки; • Усогласување на влезни податоци.
Контроли на излез	• Потврда за целосност и точност на податоците, нивно усогласување; • Преглед и следење на излезни податоци; • Надзор и следење на спроведување на апликациите-извештаи за утврдени исклучоци; • Постапки за означување, управување, чување и доставување на излезни податоци.
Контроли на безбедност на апликацијата	• Механизми за следење (ревизорска трага, преглед на најави, употреба на единствен идентификатор); • Контрола на логичен пристап до функционалности и апликациски податоци; • Заштита на складирани податоци.

Во Прилог 8 на овој Прирачник се наведени контролни цели и примери на контролни постапки кои може да ги користат ревизорите за проценка на апликациските контроли.

Ревизиите на апликациите не секогаш се од високо техничка природа. Ревизори ќе се обратат на специјализираните ревизори за ИТ во случај кога апликациските контроли се исклучително комплексни или се на високо техничко ниво, и кога нема задоволителни компензирачки контроли кај корисникот на апликацијата. Меѓутоа повеќето апликации се дизајнирани на тој начин што на раководството на субјектот му даваат доволно сигурност дека податоците и нивната обработка се правилни, без да се бара од нив да бидат експерти за информациски системи. Во такви случаи, проверките и постапките (вклучувајќи ги и постапките пропишани во прирачниците) коишто рутински се извршуваат од страна на персоналот на субјектот можат да дадат задоволителна сигурност за веродостојноста на податоците и резултатот од обработката. Во повеќето ситуации при вршењето на ревизија на информациските системи, ова ниво на сигурност ќе биде прифатливо и за ревизорите[15].

а. Контроли на влез

Целта на контролите на влез е да се осигура дека процедурите и контролите даваат разумно уверување:

[15] Европски упатства за примена на ревизорските стандарди на INTOSAI 1998, бр. 22. Ревизија на информациони системи, точка 3.8

(i) дека податоците кои треба да се процесираат се автентични, комплетни, точни и потврдени од овластено лице, и

(ii) дека податоците се внесуваат точно и без повторување. Контролата на внес е особено важна како најзначаен извор на грешка или измама во информацискиот систем. Контролите на влез се витални за интегритетот на системот.

Значаен дел од овие мерки се создаваат во фазата на развој на апликацијата, откако деловните правила ќе се дефинираат како барања за апликацијата. Иако внесот на податоци може да биде рачен или системски, грешките и пропустите можат да се намалат со добар дизајн на формата на внес, соодветна поделба на должностите во однос на настанувањето и одобрувањето на влезните документи, како и со воведување соодветни проверки за веродостојност, точност и целосност.

Елементи на контрола на влез	Опис
Проверки на влезни податоци (валидност, целосност – проверки на двојно внесување)	Автоматизирани проверки на валидноста на внесените податоци (на пр. датумот на фактурата не е во рамки на период за кој се однесува); проверки за целосност за да се утврди дека сите клучни информации за трансакцијата се внесени (на пр. полињата за внесување на датум на фактура, име на добавувач, броеви за негова идентификација се задолжителни); проверки за двојно внесување со споредување на новите трансакции со претходно внесените (на пр. проверување на двојни фактури).
Управување со изворни документи	Документирање на процедурите за подготовка на изворните документи; распределување на изворните документи; означување на изворните документи (следливост); постапки за чување документи.
Постапки за справување со грешки	Постапка со одбиени внесови на податоци (на пр. пораки за грешки, последователни мерки за корекција, инструкции за повторен внес на податоци, употреба на привремени датотеки).
Правила за овластување за внес на податоци	Постапки за одобрување од повисоко ниво за внес на податоци од формулари. На пр. царинската декларација е одобрена од страна на претпоставениот пред истата да се внесе од вработениот за обработка во апликацијата за царина.

6. Контроли на обработка

Целта на мерките за контроли на обработка подразбира заштита на интегритетот, валидноста и веродостојноста на податоците и заштита од грешки во текот на циклусот на обработка на трансакциите – од прием на податоците од потсистемот за внес до испраќање на податоците во база на податоци, известување или потсистемот за излез. Овие мерки обезбедуваат валидните влезни податоци да се обработат само еднаш, а откривањето погрешни трансакции да не ја прекинува обработката на валидните трансакции. Со тоа се зголемува веродостојноста на апликациските програми во насока на исполнување на барањата на корисниците.

Контролните постапки подразбираат да се воспоставуваат и воведат механизми за овластување на почеток на обработка на трансакциите и да обезбедат користење

само на соодветни и овластени апликации и алатки. Тие рутински потврдуваат дека обработката е извршена комплетно и точно со автоматизирани контроли.
Контролите може да подразбираат и проверка и утврдување на грешки во редоследот на внесување и двојни внесувања, бројот на трансакции/датотеки, референцијални проверки на интегритет, контролни збирови и збирови за споредба, проверки на опсегот и прекумерна резервирана меморија (buffer overflow).

в. Контроли на излез

Целите на контролите за излез се да се вградат мерки во апликацијата со цел излезните податоци од трансакцијата да бидат комплетно, прецизно и точно испорачани. Тие ги заштитуваат обработените податоци од неовластени измени и пренесувања.
Контролните процеси подразбираат соодветно дефинирање излезни податоци, очекувани извештаи утврдени во фазата на дизајн и развој на системот, соодветна документација за логичко издвојување податоци, контроли кои го ограничуваат пристапот до обработените податоци, преглед на излезни податоци, усогласување и проверка.

г. Контроли за безбедност на апликацијата

Контролите за безбедност на апликацијата подразбира одржување на доверливост, интегритет и достапност на информации во рамки на апликацијата. За цели на ревизијата, важно е да се разберат меѓусебните врски т.е. различните извори на влезни и излезни податоци во апликацијата и начинот на кој податоците се складираат.
Во повеќето апликации се пристапува со индивидуални кориснички податоци и лозинки. Сепак, и други форми на регистрирање како што е механизмот за единствена најава стануваат сè поактуелни, особено ако се земе предвид огромниот број апликации кои се користат во работната средина. Пред сè, треба да се разбере дизајнот на апликацијата во однос на овластувања на корисниците. Ревизорот ќе треба да ги провери политиките и постапките на субјектот за давање и одземање пристап на корисници, со цел да се разбере степенот до кој правилата за пристап се вградени во секое апликациско ниво и да се обезбеди дека апликацијата има контроли за давање и одземање на пристап.
Со цел да се разберат постапките за контрола на безбедноста на апликацијата, ревизорот треба да ги запознае учесниците, улогите и обврските на инволвираните во апликацијата, како на пр. администратори, напредни корисници, редовни корисници итн. Дизајнот на контролниот модул за логички пристап може да биде различен. Повеќето софтвери вршат проверка на комбинација од кориснички идентификациски податоци и лозинки пред да дозволат пристап. Пристапот може да се контролира за секој модул или опција на мени, секој прозорец или да биде контролиран преку атрибути и улоги. Ревизорот треба да го провери дизајнот на модулот за контрола на пристап имајќи го предвид значењето на тековните функции/активности. Понатаму, неопходно е да се препознаат механизмите за

обезбедување запис и хронологија на трансакциите како и да се заштитат складираните податоци во апликацијата.

Следува листа со примери за ревизорски прашања за контроли за безбедност на апликацијата:

- Хронологија на трансакции: регистрација на трансакции; употреба на единствени кориснички идентификациони податоци; известување и надгледување на записи; во идеален случај логовите треба ги регистрираат сите изменети датотеки или полиња, периодот на настанатата измена, што се променило, во што се променило и кој ја извршил промената.
- Профили на корисници, дозволи и управување со лозинки: употреба на гостински, тест и општи профили; употреба на привилегирани и администраторски профили и дополнителни контроли; постапки за давање и одземање пристап; постапки за престанок на работно место и одземање пристап; усвојување на принципот за најмала привилегија; пристап на ИТ/развојниот тим до податочни бази во продукција, формални постапки за одобрување и доделување пристап; употреба на сложени лозинки; повремени промени на лозинките; кодирање лозинки итн.
- Заштита на главните датотеки и тековните податоци: контроли за да се утврди дека измените на тековните податоци се од овластено лице; корисниците се одговорни за секоја настаната промена; тековните податоци се ажурирани и прецизни, а интегритетот на главните датотеки е сочуван. Примери на тековни податоци: детали за добавувачи и клиенти (име, адреса, телефон, број на сметка); стапки на инфлација; податоци за администрација на системот како што се датотеки со лозинки и дозволи за контрола на пристап итн.
- Конфликтни задачи и поделба на должности: различни кориснички улоги; права за пристап достапни за секој кориснички профил; правила за поделба на должности.

Ризици за субјектот на ревизија

Последиците од пропустите на апликациските контроли зависат од природата на деловната апликација. Ризиците варираат од незадоволство на корисникот до вистински катастрофи и загуби. На пример, довербата на граѓаните во државните услуги може да се намали; отсуството на сообразност со законските стандарди може да доведе до судски спор; електричната енергија може да не стигне до домовите на граѓаните; банкарските сметки може да бидат подложни на измама итн.

Попрецизно кажано, значајните ризици кои најверојатно настанале во отсуство на соодветни контроли на влез се ризик од погрешна обработка, па апликацијата нема да успее да ги оствари деловните цели. Податоците кои се обработуваат од страна на апликацијата може да бидат недоследни, па апликацијата ќе понуди несоодветни излезни податоци. Понатаму, дури и да постојат такви контроли, можно е нивно заобиколување во специфични ситуации. Во таков случај, мора да постојат дополнителни контроли како записи и правила за одобрение зошто во спротивно, предефинираната привилегија може да биде злоупотребена и да доведе до недоследни податоци во апликацијата.

Постапките за управување со изворни документи и одобрување на внес на податоци се исто така важни контроли на влез. Во отсуство на правилно раководење со изворните документи, можеби нема да биде возможно да се следи изворот на информациите внесени во системот, можеби нема да се постигне усогласеност со регулативата, а политиките за чување можат да не се почитуваат и во апликацијата да се внесуваат неверодостојни податоци. Од друга страна, во отсуство на контроли за одобрување на внес, неовластените податоци може да доведат до грешки или измама.

Пропустите во контролите за обработка може да доведат до грешки во обработката и неможност да се остварат целите за апликацијата. Тие настануваат поради погрешно мапирање на деловните правила, неадекватно тестирање на програмскиот код или несоодветна контрола на различните верзии на програмите со цел повторно да се воспостави интегритетот на обработката по појавата на проблем или неочекуван прекин. Во отсуство на неопходни контроли на обработката, можно е повторување на погрешни трансакции кои би имале влијание врз целите и угледот на субјектот.

Кај системите за обработка во реално време, некои од контролните мерки како што е усогласувањето на вкупните влезни и излезни податоци со цел да се потврди целосноста на влезните податоци и чувањето одредени оригинални документи како ревизорска трага, не се достапни. Сепак, системите во реално време вклучуваат други дополнителни контроли во рамките на апликацијата како што се интерактивно комплетирање податоци, инструкции за валидација, регистрација на обиди за пристап итн.

Недостигот на соодветна контрола за излез на податоци води до ризик од неовластена измена/бришење на податоци, креирање на погрешни извештаи за раководството и непочитување на доверливоста на податоците. Понатаму, ефектот од создавањето погрешни излезни податоци ќе зависи од начинот на кој тие информации понатаму ќе се искористат во субјектот.

Во однос на безбедноста на апликацијата, недостигот на механизми за регистрација може да го оневозможи следењето и утврдување на лицето кое го предизвикало негативното однесување. Исто така, свесноста на корисникот дека постојат постапки за проверка на регистрирање и механизми за пријавување може да го намали ризикот од злоупотреба на информациските системи. Тековните грешки во податоците имаат значајно влијание врз апликацијата бидејќи овие податоци може да се искористат за голем број други трансакции во апликацијата.

Впрочем, ризиците од несоодветно управување со информацискатa безбедност можат да бидат уште поголеми. Тие може да предизвикаат повеќе последици со различен степен на сериозност: загуба на приходи, необезбедени услуги, загуба на кредибилитетот, застои во деловната активност, правни последици, судски спорови, злоупотреба на интелектуална сопственост итн. Повеќе за ризиците и контролите за ублажување е дадено во поглавјето за информациска безбедност.

Ревизорска програма

Ревизорската програма за овој дел може да се најде во Прилог 9 - Ревизорска програма за ревизија на апликациски контроли

2.6.8. Дополнителни теми од интерес

Постојат голем број нови области во ИТ кои можат наскоро да станат предмет на ревизија. За да може успешно да спроведе ревизија на такви теми ревизорот треба да е запознаен со нив. Иако овие области може да имаат технички специфичности или посебни аспекти, сепак можат да се ревидираат со помош на истите пристапи и техники кои се разгледуваат во овој прирачник. За секој посебен тип ревизија, ќе постои потреба од дополнителни ревизорски прашања/проблеми/прашалници кои ревизорот треба самостојно да ги развие при работењето со вакви области и тие ќе зависат од ревизорските цели.

Интернет страни/портали

Интернет страните се информациски системи лоцирани на интернет или интранет и нудат услуги и содржини како текстови, слики, видео и аудио снимки и сл. Интернет порталот ги организира информациите од различни извори на еднаков начин со што се овозможува доследен изглед и впечаток. Најчесто, интернет порталите нудат услуги од типот на интернет пребарувачи, вести, информации, пристап до системи, податочни бази и забава.
Области на ревизија кои би можеле да бидат опфатени се:

- искуство на корисници;
- безбедност, приватност;
- време на одговор и
- ангажирање надворешни соработници за поврзани прашања.

Мобилно компјутерство

Сè повеќе расте бројот на услуги кои јавноста ги добива преку секакви видови ИТ комуникации. Ова се однесува на употребата на безжични комуникациски технологии за овозможување апликации и информации. Денес, во мобилната средина се нудат голем број апликации. Мобилни телефони, таблети, безжични мрежи, телевизори и многу нови електронски уреди и алатки се користат за добивање информации. Мобилното компјутерство може да се сфати како точка на ИТ пристап (персонален компјутер, лаптоп и сл.), но тука се сретнуваат и некои посебни области на ревизија кои може да се од посебна важност.
Области на ревизија кои би можеле да бидат опфатени се:

- безжична безбедност, приватност, кодирање;
- искуство на корисници;
- посебни политики во однос на мобилното компјутерство во субјектот;
- ризици од користење лични уреди за пристап до службените податоци и услуги;
- ризици од неовластен пристап до податоците на уредите;
- зголемени ризици од штета или кражба на службените уреди.

Компјутерско форензичка ревизија

Форензичката ревизија е ревизија која се врши за испитување дигитални медиуми како техника во однос на собирање на докази за одредена состојба. Зачувувањето докази е задолжително во текот на компјутерско - форензичката анализа. Тоа подразбира пристап, алатки и техники за испитување дигитални информации со цел идентификација, зачувување, обновување, анализирање и претставување факти и мислења за складираните информации.
Области на ревизија кои би можеле да бидат опфатени се:

- задржување докази за анализа (податоци, пристап, записи);
- снимање и зачувување на податоци за престапот што е можно поблиску;
- стандарди за собирање податоци за можна примена во правна процедура;
- минимална вклучена постапка за прибирање податоци без нарушување на деловните операции;
- идентификација на натрапници, доколку е можно.

Електронска влада, електронско управување и мобилно управување (eGov, e-Gov и m-Gov)

Развојот на информатичката технологија значајно го промени начинот на кој државните институции им нудат услуги на граѓаните. Како што технологијата се шири меѓу населението, тие се засегнати со нови методи на давање информации и апликации кои му користат на населението. Електронска влада, електронско управување (познато како eGov или e-gov) и мобилно управување се некои области блиски до оваа тема. Концептите се поврзани, но не се целосно слични.
Области на ревизија кои би можеле да бидат опфатени се:

- од субјектите да се бара да понудат услуги на економичен, ефикасен и ефективен начин.
- давањето електронски услуги овозможува широк опсег по прифатлива цена.

Од ревизорска перспектива, ревидирањето информациски системи или деловни процеси вклучени во e-gov или m-gov стратегијата не се разликува од стандардната ИТ ревизија. Ревизорот треба да ги разгледа дополнителните политики и механизми за спроведување (на пример, политика на субјектот за мобилно компјутерство, софтвер за кодирање, ограничување на употреба на паметни телефони за лични потреби, итн.).

Електронска трговија (Е-трговија)

Електронската трговија (Е-трговија) се однесува на секаков вид работење или комерцијална трансакција направена преку интернет мрежа. Таа вклучува, но не е ограничена на, продажба и тргување со информации, добра и услуги.
Голем број технологии и деловни процеси денес се поврзани со е-трговија: портали, трансфер на електронски (средства) финансии, онлајн банкарство, управување со ланец на достава, маркетинг, онлајн купување, мобилна трговија, управување со залихи, итн.

Постојат неколку аспекти клучни за системот на е-трговија кои како области на ревизија би можеле да бидат опфатени:

- достапност,
- безбедност на трансакции,
- приспособливост на решенијата,
- искуство на корисниците и најважното,
- деловниот процес опфатен со стратегијата за е-трговија.

3. ИТ РЕВИЗИЈА КАКО РЕВИЗИЈА НА УСПЕШНОСТ

Ревизијата на успешност се состои од следните последователни четири фази:

- Планирање,
- Извршување,
- Известување и
- Следење на спроведување на препораките.

Фаза планирање ја сочинуваат два главни чекори:

- Процес на избирање на теми на ревизијата и
- Дизајнирање на ревизијата

Процес на избирање теми на ревизијата е дел од **процесот на стратешко планирање** на ревизијата, каде се анализираат потенцијалните области и се врши истражување, со цел да се утврдат ризиците и проблемите. Голем е бројот на можни теми и програми. При изборот на тема треба да се имаат предвид ограничувањата за спроведување на ревизиите во смисла на расположливи капацитети како човечки и финансиски ресурси, временската рамка и професионалните вештини. Кога се избира темата за ревизија треба да се земат предвид можните влијанија што ќе ги има таа ревизорска тема во обезбедување на користи за управувањето со јавните финансии, субјектот предмет на ревизија или заинтересираната јавност.

Дизајнирање на ревизијата претставува клучен чекор во планирањето на ревизија на успешност и ќе помогне за стекнување на потребното знаење за извршувањето на ревизијата. Дизајнирањето на ревизијата е важен дел за спроведување на контрола на квалитет во ДЗР.

Фаза извршување - претставува собирање и анализа на податоци и информации за да се обезбедат доволно и соодветни ревизорски докази со цел утврдување наоди, донесување заклучоци како одговор на ревизорските цели и прашања, како и давање на применливи препораки кога е соодветно.

Фаза известување - претставување на резултатите од ревизијата со изработка на извештај од извршената ревизија на успешност. Извештајот треба да му овозможи на читателот да разбере зошто и како ревизијата била спроведена и да понуди практични препораки кои ќе овозможат корисни промени во управувањето со средствата, програмите и активностите. Професионалниот пристап на државната ревизија се гради преку јасни концизни и навремени извештаи кои придонесуваат кон подобрување на економичноста, ефикасноста и ефективноста при користењето на јавните средства и ресурси. Ревизиите на

успешност се вообичаено ангажмани со директно известување. Во случај на ангажмани со директно известување, ревизорот е тој што го мери или оценува предметот на ревизијата според критериумите. Во овој тип на ангажман, ревизорот не дава експлицитна изјава за уверување за предметот на ревизијата. Во такви случаи, ревизорот за корисниците обезбедува неопходно ниво на уверување на начин што дава јасно и прецизно објаснување како се изработени наодите, критериумите и заклучоците на балансиран и разумен начин, како и причината зошто комбинацијата на наодите и критериумите резултира со севкупниот заклучок или препорака.

Следење на спроведувањето на препораките (follow up) - има за цел да утврди дали преземените активности од страна на субјектот или на друга одговорна страна, како одговор на наодите и препораките ги решиле предметните проблеми и / или слабости. Следењето не е ограничено само на спроведувањето на препораките, туку се фокусира на тоа дали субјектот соодветно пристапил кон проблемите и ја подобрил утврдената состојба во разумен временски период. При следење на постапувањето по препораките од ревизорскиот извештај, ревизорот треба да се фокусира на наодите и препораките кои сè уште се релевантни во тој момент и да има непристрасен и независен пристап.

Во процесот на ревизијата на успешност важно е да се вклучат размислувањата за влијанието од самата ревизија. Ова може да се направи со тоа што ќе се одговорат неколку главни прашања во фазите на ревизијата на успешност:

- Какво е очекуваното влијание од оваа ревизија на успешност?
- Дали избраната тема ќе придонесе да се постигне посакуваното влијание од ревизијата?
- Дали дизајнирањето на ревизијата ќе доведе до постигнување на посакуваното влијание од спроведувањето на ревизијата?
- Дали заинтересираните страни се вклучени за време на целиот ревизорски процес?
- Дали препораките дадени со ревизијата ќе доведат до позитивно влијание, вклучувајќи ги ранливите категории (инклузивност)?
- Дали на заинтересираните страни им се пренесени главните пораки?
- Дали се создадени услови за соодветен follow-up и имплементирање на препораките?

Поодделните специфичности, карактеристични за секоја фаза кај ревизијата на успешност се обработени и ќе се применуваат од Прирачникот за ревизија на успешност.

4. ИТ РЕВИЗИЈА КАКО РЕВИЗИЈА НА УСОГЛАСЕНОСТ

Ревизијата на усогласеност е проценка за тоа дали се почитуваат одредбите од важечките закони, правила и прописи изготвени според законите и различните наредби и упатства издадени од надлежен орган. Оваа ревизија по својата природа промовира одговорност, добро владеење и транспарентност. Императив е ревизиите на усогласеност да се планираат, спроведуваат и известуваат на структуиран начин.

Ревизијата на усогласеност може да се спроведе како самостојна ревизија или како ревизија комбинирана со финансиска ревизија и/или ревизија на успешност. Ревизијата на усогласеност најчесто се извршува како самостојна активност според барањата и објаснувањата од ISSAI 4000. Стандардот за ревизија на усогласеност ISSAI 4000 се заснова на основните принципи во ISSAI 100 и 400.

Процесот на ревизија на усогласеност ги опфаќа следните фази и активности.

Планирање на ниво на ВРИ: Во фазата на планирање на ниво на ВРИ, ВРИ ја избира темата и подготвува годишен план за ревизија на усогласеноста. ВРИ одлучува дали ангажманот ќе биде со потврдување (атестирање) или со директно известување и дали со разумно или ограничено уверување. ВРИ ги зема предвид принципите од етичко значење - т.е. независност и објективност на ревизорот, компетентност на тимот и гарантира дека постојат процедури за контрола на квалитетот. ВРИ, исто така, се погрижува тимот да може да ја спроведе ревизијата со потребната документација и комуникација во текот на целиот период. Државниот завод за ревизија најчесто извршува ревизии на усогласеност како ангажман за директно известување со разумно уверување.

Планирање на индивидуална ревизија: Во фазата на планирање, ревизорот ја разгледува врската помеѓу предметот, критериумите и опфатот на ревизијата за усогласеност. Ревизорите се водени од професионалното расудување и потребите на наменетите корисници додека ја извршуваат оваа фаза. Откако ќе одлучат за предметот, критериумите и опфатот на поединечниот ангажман за ревизија на усогласеноста, тие ја разработуваат ревизорската стратегија и планот за ревизија. Тие ја разбираат внатрешната контрола, утврдуваат материјалност, ги проценуваат ризиците за ентитетот и планираат ревизорски процедури како дел од дизајнирањето на ревизијата.

Спроведување на ревизија и собирање докази: Во оваа фаза, ревизорите примарно собираат и документираат докази за да формираат заклучок или мислење за тоа дали предметот, во сите материјални аспекти, е во согласност со утврдените критериуми. Во некои случаи, ревизорите можеби ќе треба да го променат опсегот на ревизијата на усогласеност доколку наидат на ревизорски докази кои укажуваат на потреба од таа промена. На пример, додека собираат докази, ако ревизорите пронајдат нешто што укажува на измама, можеби ќе треба да ги изменат своите процедури. Кога ќе се

идентификува можноста за измама, ревизорите преземаат активности за да се осигураат дека соодветно реагираат и ќе треба да документираат зошто го промениле својот план за ревизија. Иако ревизијата може да дејствува како спречување на измама, таа вообичаено не е дизајнирана да открие измама[16].

Оценување на доказите и донесување заклучоци: На крајот од ревизијата, ревизорите ги испитуваат доказите за доволност и соодветност со цел да формираат заклучок или мислење дали предметот е усогласен со утврдените критериуми. Во оваа фаза, ревизорите ја земаат предвид материјалноста за потребите на известувањето.

Известување: Заклучокот или мислењето се презентираат во форма на извештај до наменетиот корисник. Овде ревизорот ги вклучува препораките и одговорите на субјектот на нив.

Следењето на спроведувањето на препораките (follow up), има за цел да утврди дали преземените активности од страна на субјектот или на друга одговорна страна, како одговор на наодите и препораките ги решиле предметните проблеми и / или слабости. Следењето не е ограничено само на спроведувањето на препораките, туку се фокусира на тоа дали субјектот соодветно пристапил на проблемите и ја поправил утврдената состојба во разумен временски период.

При следење на постапувањето по ревизорскиот извештај, ревизорот треба да се фокусира на наодите и препораките кои се сè уште релевантни во тој момент и да има непристрасен и независен пристап.

Овие фази со поодделните специфичности, карактеристични за секоја фаза кај ревизијата на усогласеност се обработени и ќе се применуваат согласно Прирачникот за ревизија на усогласеност.

[16]ISSAI 4000.63

5. СПЕЦИФИЧНИ ТЕХНИКИ ВО ИТ РЕВИЗИЈА/ СПЕЦИФИКИ И ТЕХНИКИ ВО ИТ РЕВИЗИЈА

Специфики за ИТ ревизијата

Во истражувањето вклучуваме испитување на информациските системи со анализа на: законски и подзаконски акти, интерни акти и стратегии, стандарди, соодветна литература, документи, интервјуа, користење на експертизи, анализирање на индикации за потенцијални проблеми од аспект на постигнување на организациските цели и ефикасно искористување на ресурсите (планирање на ресурсите на субјектот, безбедност на информациските системи, набавка на софтверски апликации, развој на системи и континуитет на истите итн.).

При утврдување на опфатот, ревизорот треба да има предвид дека јадрото на ИТ системот кај субјектот најчесто претставува комбинација од:

- систем за управување со конкретни бази на податоци;
- апликациски софтвер(и) кој ги одредува правилата на работење во системот преку посебни модули и
- кориснички интерфејс поддржан од мрежен апликациски софтвер, доколку постои мрежно опкружување.

Базите на податоци и апликацискиот софтвер се лоцирани на сервери (компјутери со голем капацитет на кои може да се постават голем број бази на податоци и апликации). Серверите можат да бидат различни во зависност од барањата на корисниците, на пример сервери за податоци (data servers), апликациски сервери (application servers), интернет сервери (internet servers) и прокси сервери (proxy servers).

За прибирање на потребните информации и стекнување со потребните знаења можат да се применуваат најразлични постапки и техники. Пристапите, моделите и методите кои се користат варираат од ревизија во ревизија. Во зависност од барањата, ревизорите може да користат било која од следните техники:

- вадење/издвојување/извлекување податоци преку добивање копија од податоците од субјектот на ревизија. Ревизорот можеби ќе треба да создаде слична средина како таа на субјектот на ревизија (оперативен систем, систем за управување со бази на податоци, хардвер, итн.) за да изврши анализа/издвои/повлече податоци од копијата на податоците. Од ревизорот може да се побара да ги конвертира податоците од една во друга форма за полесно читање и анализа.
- употреба на ревизорски софтвер за вадење/издвојување/извлекување податоци од разни комбинации на оперативни системи, системи за управување со бази на податоци, апликациски системи, итн. ИТ ревизорите може да користат општ или

посебен ревизорски софтвер. Општиот ревизорски софтвер може да се користи и во специфични индустрии или може да биде помошен софтвер (utility software) за оценка на функционирање на различните алатки (utilities) на информациските системи. Употребата на некоја од нив или нивна комбинација ќе зависи од целите и опфатот на ИТ ревизијата.

- тестирање податоци во ситуации кога е потребно тестирање на квалитетот на програмата. Претпоставката е дека е возможно да се генерализира за севкупната веродостојност на програмот кога таа е веродостојна за група специфични тестови. Оваа техника подразбира дизајнирање тест податоци и креирање тест податоци пред да се започне со употреба на програмата со тест податоци.

Исто така, субјектите на ревизија имаат сопствена комбинација на хардвер, оперативен систем, системи за управување со бази на податоци, апликациски софтвер, мрежен софтвер, итн. ИТ ревизорите треба да се способни да соберат информации од овие извори со цел да извршат нивна анализа. Запознавањето на ИТ системот и базите на податоци во субјектот е суштински чекор во прибирањето податоци.

Ревизорите треба да одлучат за соодветноста на употребата на една или повеќе техники за прибирање на податоци, како и да се уверат во интегритетот на податоците и користа од истите. Употребата на било која од техниките не треба да влијае врз интегритетот на апликацискиот систем и неговите податоци во субјектот на ревизија.

Техниките за прибирање податоци треба да се засноваат врз проценки на ризик и повратни ревизорски резултати кои се очекуваат да се добијат со соодветни техники, како и расположливото време и ресурси за ревизијата.

Ризикот е веројатност дека одреден настан или активност може негативно да влијае на субјектот, односно оневозможување на постигнување на целите на субјектот и ефикасно искористување на ресурсите, рефлектирано преку несоодветно планирање на ресурсите, загрозена безбедност на информациските системи, несоодветни набавки на хардвер и софтвер, или општо – загрозување на континуитетот на субјектот.

Проценатa на ризиците вклучува проценување на:

- фактори кои со своето постоење и влијание го отежнуваат доброто управување, без разлика колку субјектот се труди да го постигне, и
- колку се добри контролите при управување со субјектот, програмата тема на ревизија.

Врз основа на проценка на ризик, опфатот на ревизијата на ИС може да се извлече од една или повеќе области за ревизија.

При обезбедување на податоците **неопходни за вршење на ИТ ревизија** во случај на прием на префрлена голема количина на податоци[17] од субјектот на ревизија, ревизорите може да осигурат дека секоја префрлена голема количина на податоци е придружена со писмо од субјектот на ревизија. Таквото пропратно писмо може да го прецизира следното:

- Изворот на податоците (преку упатување на временскиот печат генериран при префрлањето на податоците / хаш број за префрлање на податоци) за обезбедување интегритет на податоците, проверка на автентичноста[18] и непобивање[19]
- Параметрите за екстракција користени за креирање на префрлена голема количина на податоци, на пр. користени пребарувања (queries) / стартувани извештаи.
- Доколку такво пропратно писмо не е примено од субјектот на ревизија, може да се генерираат интерни документи од ревизорите во кои ќе бидат наведени важни информации, како на пр. датумот на предавање на податоците, од која датотека е креирано префрлањето на податоци, и дали податоците се од продукциска околина или од некоја друга околина итн.

Ревизорите можат да осигурат дека собраните и документирани електронски докази се доволни, сигурни и точни за прифаќање на заклучоците на ревизијата. Вакви електронски докази може да бидат датотеки со податоци, дневници на корисници (кориснички логови), аналитички модели, извештаи за управување со информациски системи итн., а тие може соодветно да се соберат и складираат на начин да бидат достапни за да се обезбеди уверување за точноста и валидност на ревизорскиот процес. Доказите собрани за време на ревизијата на ИС може да имаат временски ознаки (време на обезбедување на податокот) и детали кои ги содржат чекорите на извршување на анализата на податоците, така што јасно ќе се знае кога доказите биле креирани, складирани и последен пат изменети, за да се намали ризикот од последователни промени.

Ревизорите можат да осигурат дека собраните и документирани електронски докази се доволни, сигурни и точни за прифаќање на заклучоците на ревизијата. Вакви електронски докази може да бидат датотеки со податоци, дневници на корисници (кориснички логови), аналитички модели, извештаи за управување со информациски системи итн., а тие може соодветно да се соберат и складираат на начин да бидат достапни за да се обезбеди уверување за точноста и валидност на ревизорскиот процес. Доказите собрани за време на ревизијата на ИС може да имаат временски ознаки (време на обезбедување на податокот) и детали кои ги содржат

[17] Data dumps - Префрлени податоци се дефинирани како голема количина на податоци пренесени од еден систем или локација на друга

[18] Автентикацијата е дефинирана како акт за проверка на идентитетот на корисникот - Поимник на условите на ISACA

[19] Непобивањето се дефинира како уверување дека страната подоцна не може да го негира потеклото на податоците; обезбедување
доказ за интегритетот и потеклото на податоците кои може да се проверат и од трето лице - Речник на термини на ISACA

чекорите на извршување на анализата на податоците, така што јасно ќе се знае кога доказите биле креирани, складирани и последен пат изменети, за да се намали ризикот од последователни промени.

Ревидирање на компјутерска програмата (Program review)

Ревидирање на компјутерската програма се користи како техника за потврда на валидноста на процесите во компјутерските програми. Ревидирање на компјутерската програма подразбира читање на програмските кодови од страна на ревизорот за да се утврди следното: погрешен код, неавторизиран код, неефективен код, неефикасен код и употреба на нестандарден код.
Ревидирањето на програмата се врши преку следните чекори:

- Селекција на компјутерска програма што треба да се ревидира;
- Ревидирање на програмските стандарди на инсталацијата;
- Разбирање на програмската спецификација;
- Обезбедување дека изворниот код е тој што се користи;
- Ревидирање на програмскиот јазик користен за компјутерската програмата;
- Ревидирање на изворниот код и
- Утврдување на импликациите од недостатоците и неефикасностите.

Со оваа техника се обезбедува осигурување дека програмата функционира како што е специфицирана, се обезбедува заштита од измами, може да се верификува усогласеноста со програмските стандарди и може да ги утврди неефикасните компјутерски програмски кодови.

Споредба на кодови

Споредба на кодови се користи како техника за потврда на валидноста на процесите во компјутерските програми. Оваа техника вклучува споредба на две верзии од програмскиот код – верзијата која ја добил ревизорот и верзијата која ја користи субјектот. Ревизорот ја користи оваа техника да провери дали софтверот што му е обезбеден за ревизија е истиот што се употребува и да провери дали биле направени промени во кодот во претходни верзии и ако биле, дали биле проследени соодветни процедури за управување со промени.
Оваа техника може да биде единствена прифатлива техника за верификација на автентичноста на софтверот што го ревидира ревизорот. Кај оваа техника софтверските алатки се достапни за споредби и се релативно лесни за употреба. Истата претставува брз начин за утврдување на неавторзираните кодови и можни измами.

Паралелна симулација

Паралелна симулација се користи како техника за потврда на валидноста на процесите во компјутерските програми. Паралелната симулација вклучува создавање на независен сет на кодови кои ја имитираат функцијата на тестираната

област. Резултатите може да се споредат со оние што се произведуваат од самата апликација. Паралелната симулација е корисна алатка што му овозможува на ревизорот да ја оцени успешноста на целата или дел од апликацијата што се тестира. Обично, ова се врши во областа на апликацијата која е предмет на ревизорски интерес. Ова е добар начин да се докаже точноста на пресметките и процедурите за обработка во системот без да има влијание на системот. Ревизорот ќе треба да има добро знаење за системот и за процедурите што ќе ги реплицира, како и искуство во програмирање.
При користење на оваа техника ревизорот треба да поседува вештини во програмирање, детално знаење на програмскиот код што ќе се тестира и добро разбирање на процедурите што треба да се реплицираат. Притоа треба да се има во предвид дека оваа техника одзема многу време и ресурси.

Тест податоци

Тест податоци се користи како техника за потврда на валидноста на процесите во компјутерските програми. Тест податоци подразбира ревизорот да користи примерок за да оцени дали постојат логички грешки во програмата и дали програмата ги исполнува целите. Се заснова на заклучокот дека програмата е во целост веродостојна, доколку специфичните тестови се веродостојни.
Терминот „тест податоци" обично е резервиран за техника каде сет на тестови е дизајниран наместо заснован на сет на постоечки податоци. Со други зборови, пристапот со тест податоците се креира да тестира специфични аспекти на програмата.
Со оваа техника се обезбедува позитивно осигурување за точното функционирање на контролите. Како недостатоци на оваа техника се високите почетните трошоци за воспоставување и можното влијание врз датотеките на апликацијата.

Трага

Трага се користи како техника за потврда на валидноста на процесите во компјутерските програми. Трагата му овозможува на ревизорот да го анализира секој чекор во компјутерската програма. Оставајќи трага можно е да се види како секоја линија на кодот има влијание врз податоците што се обработуваат или на самата програма. На пример, ако програмата не дава точни збирови, со оваа техника се утврдува грешката.

Софтвер за испитување на датотека

Софтвер за испитување на датотека се користи како техника за анализа на датотеки со податоци, која индиректно му помага на ревизорот да донесе заклучоци за квалитетот на програмата. Испитување на датотека вклучува различни тестови кои се вршат на датотеката како проверка на контролните збирови, двојни влезни податоци, влезни податоци што недостигаат, невообичаени трансакции, примероци, итн. Тестовите може да се извршат со SQL, програми специфични за

системот што се ревидира или со користење на генерализиран ревизорски софтвер. Како најраспространети софтвери се ACL и IDEA. Овие алатки ја подобруваат ефикасноста на ревизорската работа.
Оваа техника може да се користи за:

- тестирање на податоци обезбедени до различни ИТ системи,
- тестирање на големи примероци или на цела популација многу ефикасно,
- обезбедува различни функции на едно место за ревизорски цели и
- автоматски ги документира резултатите на ревизорските тестови.

Во Државниот завод за ревизија се користи IDEA софтверот.

SCARF (The system control audit review file (SCARF technique))

SCARF техника се користи како техника за анализа на датотеки со податоци, која индиректно му помага на ревизорот да донесе заклучоци за квалитетот на програмата. SCARF техника вклучува интегрирање на модули на ревизорски софтвери во рамките на апликациониот систем – за да обезбеди континуиран мониторинг на системските трансакции. Овие ревизорски модули се поставени на претходно утврдени точки за да прибираат информации за трансакциите кои се од интерес за ревизорот. Тие информации потоа се впишуваат во специјален ревизорски фајл наречен SCARF master file. Периодично, ревизорот ги проверува информациите содржани во овој фајл за да види дали некој аспект од системот треба да се преиспита.

6. СЛЕДЕЊЕ НА СПРОВЕДУВАЊЕТО НА ПРЕПОРАКИТЕ

Следење на спроведувањето на препораките (Follow up) е дел од процесот на ревизија со која се зајакнува влијанието на ревизијата и се подобрува идната ревизорска работа. Овој процес ја поттикнува ефективната имплементација на препораките од страна на субјектите опфатени со ревизијата и дава информација за Државниот завод за ревизија, законодавецот и Владата за ефективноста на ревизијата на успешност. Следењето на постапувањето по препораките треба да ја зголеми вредноста на ревизорската работа и да ги охрабри субјектите опфатени со ревизијата и другите корисници на извештајот да ги земат во предвид препораките со цел подобрување на состојбите во иднина.

ВРИ треба да извести за резултатите од нејзините follow-up активности соодветно, со цел да обезбеди фидбек до законодавецот, извршната власт, засегнатите страни и јавноста. Веродостојни информации за статусот на воведување на препораките, влијанието на ревизиите и преземените релевантни корективни дејствија, може да помогнат да се демонстрираат вредноста и користите на ВРИ[20].

[20] ISSAI 3000/138

Начин на следење на препораките

Согласно регулативата, Државниот завод за ревизија и кај овој вид ревизија го следи спроведувањето на дадените препораки според Прирачникот за следење на спроведувањето на препораките и преку Образец ИЗПМ. Образецот претставува основа за анализа на преземените мерки по дадените препораки односно дали се преземени мерки по дадените препораки, на кој начин се имплементирани поодделните препораките и кои мерки остануваат да се преземат кај одредени препораки за кои е потребен подолг временски период за нивна имплементација и/или соодветно ниво на меѓу институционална координација.

Проценка на добиените информации

По добивање на образецот ревизорот пристапува кон проценка на нивото на мерки кои субјектот/тите на ревизија ги имплементирале и оцена на степенот на нивната ефективност со цел да оцени дали ревизијата на успешност ја постигнала целта.

Проценката на преземените мерки или активности од страна на ревизорите, базирано на докази, ќе овозможи да се донесе одлука:

- Дали да се продолжи со следењето на препораките по пат на *посебна ревизија* (follow up) за следење на препораките во функција на утврдување на степенот на спроведувањето на препораките констатирани во ревизорскиот извештај за соодветната ревизија на успешност по оценка на ревизорскиот тим, а содржано во Годишната програма на Државниот завод за ревизија,
- Можност следењето на препораките да биде *дел од идна ревизија на регуларност* во дадената област, со која ќе се овозможи собирање на докази за дадените препораки со ревизијата на успешност и
- *Спроведување на ревизии односно проверки за следење на спроведувањето на препораките во ревизорските извештаи* кои се од постојан интерес и/или претставуваат значителен ризик.

Кога ангажманот за ревизија на информациски системи произлегува од еден или повеќе од главните видови на ревизија, ревизорите може да ги земат во предвид барањата за следење (follow up) на таквите ревизорски ангажмани кои се во согласност со оние за финансиска ревизија (ISSAI 200), ревизија на успешност (ISSAI 300) и ревизија на усогласеност (ISSAI 400).

7. КОНТРОЛА НА КВАЛИТЕТ И ОСИГУРУВАЊЕ НА КВАЛИТЕТ

7.1. Контрола на квалитет на ревизиите

Подобрување на квалитетот на извршените ревизии преставува стратешка определба на Државниот завод за ревизија. Државниот завод за ревизија го препознава значењето на воспоставување и одржување ефикасен систем на контрола на ревизијата за одржување на репутацијата и кредибилитет на институцијата, како и остварување на нејзиниот мандат.

Прашањето за контрола на квалитет е обработено во ISSAI 140 – Контрола на квалитет за ВРИ, заснован на клучните принципи дадени во „Меѓународните стандарди за контрола на квалитет – ISQC-1" на Меѓународната федерација на сметководители – IFAC.

Контролата на квалитет е во насока на одржување и подобрување на квалитетно и професионално извршување на ревизорската активност. Таа го поттикнува Државниот завод за ревизија да воспостави и одржува правилен систем на контрола на квалитет на целокупната работа на институцијата.

Системот на контрола на квалитет треба да биде дизајниран на начин што ќе помогне во детектирање на сите можни ризици кои влијаат на квалитетот на ревизорската активност, со цел да испорачува спроведување на ревизија со висок квалитет. За да биде ефикасен системот на контрола на квалитет, потребно е во рамките на стратешките документи и акти на Државниот завод за ревизија да се предвиди контролата на квалитет како нејзин составен и значаен дел, со единствена цел да се задржи репутацијата и кредибилитетот во исполнувањето на мандатот. Само на тој начин квалитетот ќе биде вграден во извршувањето на задачите на Државниот завод за ревизија.

ISSAI 140 – Контрола на квалитет за ВРИ е дизајниран на начин кој овозможува да се применува во системот на контрола на квалитет за целата работа извршена на Државниот завод за ревизија како ВРИ, и тоа во: финансиските ревизии, ревизиите на усогласеност, ревизиите на успешност и било која спроведена ревизорска задача. Главниот фокус на овој стандард се организациските аспекти на квалитетот на ревизија кои функционираат во Државниот завод за ревизија.

Функционирањето на системот на контролата на квалитет на ревизиите во Државниот завод за ревизија е регулирано со Упатството за контрола на квалитет на ревизиите.

7.2. Осигурување на квалитет

Осигурувањето на квалитет на ревизиите може да се дефинира како процес преку кој ВРИ го проценува системот на контрола на квалитет (дали ефективно функционира).

Согласно ISSAI 140 - Контрола на квалитетот на ВРИ, основните принципи прилагодени за ВРИ содржани во Елемент 6: Мониторинг на овој стандард, укажуваат дека:

„ВРИ треба да воспостави процес за мониторинг со цел да се обезбеди разумно уверување дека политиките и постапките кои се однесуваат на системот за контрола на квалитетот се релевантни, адекватни и ефикасно функционираат. Процесот на мониторинг треба да:

(а) вклучува постојан преглед и оценка на системот на контрола на квалитетот на ВРИ, вклучувајќи и преглед на примерок од вкупно реализираните активности;

(б) бара назначување на одговорноста за следење на процесот на лице или лица со доволно релевантно искуство и авторитет во ВРИ за преземање на таква одговорност и

(в) бара лицата ангажирани во проверката да се независни (да не учествувале во извршувањето на работите или во активностите за контрола на квалитетот на ревизијата која е предмет на проверка).

Функционирањето на системот на осигурување на квалитет на ревизиите во Државниот завод за ревизија е регулирано со посебно Упатството за осигурување на квалитет на ревизиите.

Главен државен ревизор

м-р Максим Ацевски

Број: 01-1652/1

Скопје, 26. 12. **2022 година**

8. ПРИЛОЗИ

Прилог 1 - Општ прашалник за критичноста на системот

Прилог 2 – Ревизорска програма за ревизија на ИТ управување

Прилог 3 – Ревизорска програма за ревизија на развој и набавка на ИТ решение.

Прилог 4 – Ревизорска програма за ревизија на ИТ операции

Прилог 5 – Ревизорска програма за ревизија на ангажирање надворешни соработници.

Прилог 6 – Ревизорска програма за ревизија на план за деловен континуитет и план за обновување по катастрофа.

Прилог 7 - Ревизорска програма за ревизија на информациска безбедност

Прилог 8 - Европски упатства за примена на ревизорските стандарди на INTOSAI 1998, бр. 22. Ревизија на информациони системи

Прилог 9 - Ревизорска програма за ревизија на апликациски контроли

Прилог 10 – Барање за документација

Прилог 11 - Работна белешка