ДЗР

ДРЖАВЕН ЗАВОД ЗА РЕВИЗИЈА

ПРИРАЧНИК

ЗА ИТ РЕВИЗИЈА

Скопје, април 2016

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.

Мандат на вршење на ИТ ревизија

Мандатот на ВРИ за вршење ревизија на ИТ системите е утврден во ISSAI 1 – Декларацијата на Лима, 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.

[1] Weber Ron, Information System Audit, 2011

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.
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.

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.

2.2. ИТ ревизија како дел од ревизијата на регуларност

Согласно ISSAI 100 т.23 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 т.А51 од ISSAI 1315, 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 т. А 52 од ISSAI 1315:

- 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 на кој начин утврдените состојби треба да се надминат (т. А77 од ISSAI 1315).
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 (т. А92 од ISSAI 1315).

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 ситеми како дел од ревизијата на регуларност или како посебен тип на ревизија на успешност за оценка на инфомацискиот 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

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

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.

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. РЕВИЗИЈАТА ВО УСЛОВИ НА ИТ ОПКРУЖУВАЊЕ

2.4.1. 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;
- Само одобрени ставки претставуваат влез во системот и влезните податоци се точни и целосни;

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

- 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 превземени активности во самиот систем при што за секоја настаната измена треба да има запис за идентитет на корисникот кој ја направил измената, времето на измената, 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 во согласност со МСР 300 – Планирање на ревизијата на финансиските извештаи 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 обелоденувања;
- 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, детално објаснети во т.2.2.од овој Прирачник.

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.

2.4.2.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 критериумили 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.

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:

- 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).

2.5. Области на ИТ ревизии

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

2.5.1. 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[4]. 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.

[4] 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.

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.
Организациската 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[5].

Организациската 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 организациската 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.

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

[5] COBiT 5 – Прилог Е. Мапирање на COBIT 5 со најрелевантните поврзани стандарди и рамки.

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[6].

Управување со ризик[7]

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

[6] IT Governance in Public Sector: A Top Priority – WGITA IntoIT Issue 25, August 2007.
[7] За подетален опис види Поглавје за ИТ безбедност.

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 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[8]. 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 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,

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

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.

2.5.2. 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.

2.5.3. 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 најшироко прифатените рамки за одредување, планирање, испорака и поддршка на ИТ услуги во компаниите ITIL[9].

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

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

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.

Барања за промена од корисничка група на стандардни формати
Овластување и давање приоритет од страна на работна група/тело или одборот за контрола на промени
Измени на копија на изворниот код од страна на техничкиот кадар (програмери/мрежни техничари)
Тестирање единици од страна на програмери проследено со тестирање на ниво на корисник во тест околина
Трансфер на изменетиот и тестиран софтвер во продуциска средина од страна на трето лице, документација и **преглед од раководството.**

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.

2.5.4.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**[10], 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)[11]. 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 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

[10] Outsourced IT Environments Audit /Assurance Program, 2009.
[11] Види Водич и прирачник на работната група за ИТ ревизија за ревизија на обработка во облак

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.

2.5.5. 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 поврат на 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 поврат на 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.

2.5.6. 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, информацискатa 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 информацискатa 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 информацискатa 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 информацискатa 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.

2.5.7. 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. Апликациският 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[12]. 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[13].

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, 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,

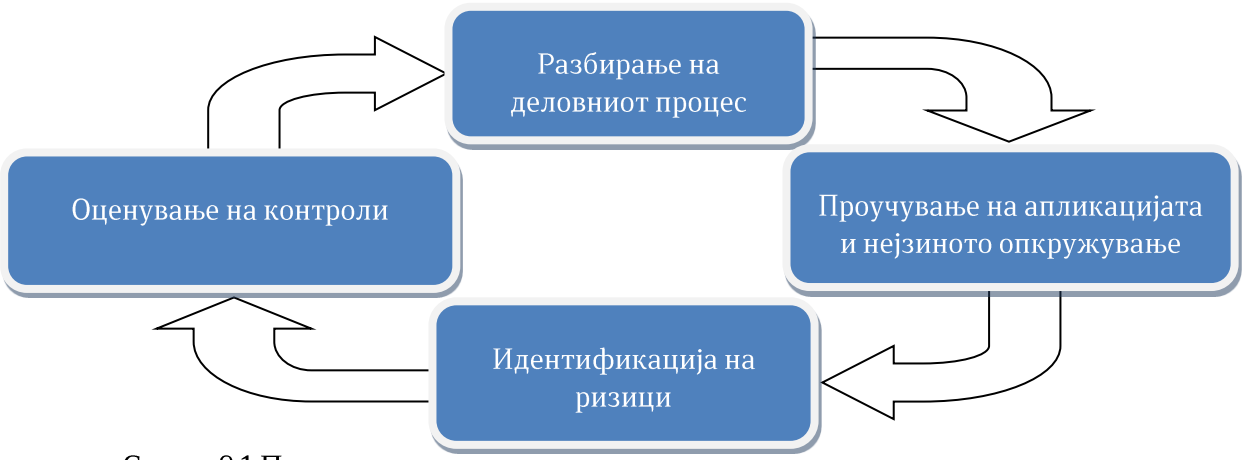
[12] ISSAI 1315, A105

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

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

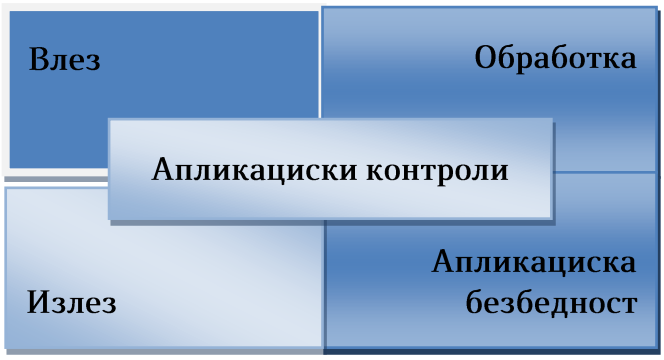
материјал. Исто така, ревизорскиот тим треба да разговара со раководителите, лицата задолжени за ИТ и клучните корисници на апликацијата.

- **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 поспецификични 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[14].

а. Контроли на влез

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

(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.

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

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

2.5.8. 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.

Во Прилог 10 на овој Прирачник се наведени примери се различните видови на теми од разни услуги и области на ревизија кои би можеле да бидат земени во предвид.

3. ИТ РЕВИЗИЈА КАКО РЕВИЗИЈА НА УСПЕШНОСТ

3.1. Планирање

Планирањето како основна фаза во процесот на ревизијата, е дел од секоја ревизија, вклучително и ИТ ревизијата.
Планирањето е динамичен процес кој го насочува процесот на извршување на ревизијата.
Фазата на планирање обезбедува информации од сегашноста и минатото, а кои се потребни за разбирање на субјектот/субјектите, програмата или проектот, со цел изградба на знаење кое секогаш вклучува истражувачки напори, проверки и анализи дали потребните податоци и докази се достапни, доволни, релевантни.
Здобивањето со потребните знаења од предметот на ревизијата е континуиран и кумулативен процес на прибирање и проценка на информациите, а кои резултираат во знаења за ревизорските докази во сите фази на ревизијата.
Планирањето ја дизајнира ИТ ревизијата како ревизија на успешност. Соодветно планирање на ревизорската работа помага да се обезбеди уверување дека доволно внимание е посветено на областите кои претставуваат интерес и предмет на ревизијата, кои потенцијални проблеми се идентификувани и дека работата ќе се заврши за најкраток временски рок. Планирањето, исто така, помага во правилното распоредување на работата на членовите на тимот и координација на работата која ја извршуваат други ревизори и експерти.
Успешното планирање, извршување на ревизијата и изразување на заклучок подразбира високо ниво на познавање на субјектот предмет на ревизија, како и финансиските, деловните и другите ризици со кој се соочува субјектот и неговите ИТ системи. ИТ системот вообичаено содржи комбинација од систем за управување со бази на податоци, апликациски софтвер кој ги одредува правилата на работењето на системот преку посебни модули, кориснички интерфејс, поддржан од мрежен апликациски софтвер, доколку постои мрежно опкружување. Базите на податоци и апликацискиот софтвер се лоцирани на сервери кои претставуваат компјутери со голем капацитет, на кои можат да се стават голем број на бази на податоци и апликации.

Планирањето на ревизијата треба да биде документирано и опфаќа:

- знаења и информации потребни за да се разбере субјектот/субјектите и неговиот/нивниот ИТ систем, проблемите, ризиците, можни извори на докази, материјалноста и значајноста на сферата на интерес на ревизијата;
- утврдување на ревизорската цел/цели, прашања/задачи, критериуми, опфат и период на ревизијата;
- техниките кои ќе бидат користени при обезбедувањето на информации и нивна анализа;
- барања поврзани со човечки ресурси, нивни компетенции како и потреба од вклучување на независни лица/експерти;
- клучни временски рамки и патокази на главните контролни точки на ревизијата, процени на евентуалните трошоци на ревизијата.

Планирањето на ревизијата е составено од: Прелиминарно истражување и изработка на Ревизорска програма.

Со *прелиминарното истражување* се утврдуваат потенцијалните цели на ревизијата, можните ризици, методологијата и пристапот на ревизијата, преку што се утврдува дали извршувањето на ревизијата е реално, разумно и каков ефект се очекува од извршувањето на ИТ ревизијата.
Со *Ревизорската програма* се утврдуваат: целта/целите на ревизијата за која се изготвува програмата; областите; ризиците; прашањата/задачите; критериумите за ревизија; опфатот; техниките за прибирање и анализа на податоци/докази; ограничувачките фактори за извршување на ИТ ревизијата; очекуваните резултати и заклучоци; временската рамка; потребните ресурси и конкретните обврски на ревизорите за остварување на поставените цели.
Многу е важно да се одлучи колку детално ќе се планира ревизијата. Доброто планирање однапред ќе спречи проблеми во ревизијата кои може да се јават во подоцнежните фази. Истовремено, многу детално планирање може понекогаш да спречи иновативно размислување. Ревизиите на информациските системи се одвиваат во комплексно опкружување и ретко може да се планираат до детали.

3.1.1. Прелиминарно истражување

Процесот на Прелиминарно истражување и активностите кои произлегуваат од него претставени се на следниот графички приказ:

3.1.1.1. Цел на прелиминарното истражување

Целта на прелиминарното истражување е да одреди дали постојат услови за спроведување на ИТ ревизијата и доколку постојат да се изготви Предлог за ИТ ревизија заедно со Ревизорска програма[15]. (Образец за ревизорска програма)

Прелиминарното истражување претставува општа проценка на ИТ опкружувањето и работењето на субјектот/субјектите опфатени со ИТ ревизијата, без да се прават детални испитувања. Во оваа фаза ревизорите прибираат информации со цел да ги појаснат почетните одлуки донесени врз основа на предлозите за ревизијата, за опфатот, временската рамка и ресурсите, како и да ги предложат целите на ревизијата, областите кои ќе треба детално да се анализираат, критериумите и ревизорскиот пристап. Ревизорскиот тим ја осмислува ревизијата на начин кој ќе го намали ризикот од невистинити согледувања и погрешни заклучоци, кои ќе обезбедат соодветно ниво на уверување.

Целта на прелиминарното истражување е:

- да се соберат информации за да се зголеми знаењето на ревизорите за темата/предмет на ревизија;
- да се идентификуваат значајните ризици;
- да се донесат заклучоци;
- да се изработи Извештај од прелиминарното истражување и Предлог за ревизија,
- да се одобри Предлог за ревизија, за продолжување со ревизијата.

Прелиминарното истражување во ИТ ревизијата вклучува испитување на информациските системи со истражување 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.).

3.1.1.2. Опфат на прелиминарното истражување

Опфатот[16] на прелиминарното истражување треба јасно да ги дефинира обемот, времето и природата на истражувањето кое треба да се спроведе. При определување на опфатот на истражувањето треба да се води грижа за рамката на активностите каде може да се добие најголема искористеност, во време и ресурси, кои се на располагање за ревизија. Опфатот на Прелиминарното истражување гарантира дека фазата на истражување е јасно ограничена.

[15] ISSAI 3000/3.3 и ISSAI 300/25
[16] ISSAI 3000/3.3/2

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 политики за примена. Утврдувањето на опфатот на ИТ ревизијата вклучува одредување на обемот на ревизорската контрола, опфатот на ИТ системите и нивната функционалност, ИТ процеси 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.

При утврдување на опфатот во прелиминарните истражува, 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).

Опфатот на прелиминарното истражување е ограничување и концентрирање на ревизијата само на неколку значајни прашања/области кои се однесуваат на темата на ревизијата. На тој начин ревизијата може да се изврши со капацитетите кои и се на располагање и се неопходни за остварување на планираните резултати.

3.1.1.3. Стекнување на потребни знаења и информации за областа на ревизијата

Прелиминарното истражување е процес каде што е можно да се тестираат/истражуваат различни идеи, алтернативни проблеми, прашања и методи. Тоа обезбедува доволно уверување за да се продолжи со ревизијата, или пак да се прекине со понатамошната работа.

Собирањето на информации[17] е важен дел од „процесот на учење" каде ревизорот се обидува да ја разбере областа што се истражува како и нејзините проблеми. Овие информации обично се собираат за да се разбере и опише предметот на ревизијата, да се измерат и оценат потенцијалните резултати, да се откријат недостатоците, да

[17] ISSAI 300/37

се опишат и анализираат односите меѓу причините и последиците, да се проверат претпоставките и аргументите.

Во прелиминарното истражување 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.

Покрај претходно наведените техники, ревизорот може да ги користи и стандардните техники од ревизијата, како и техниките кои се содржани во поедините области за ИТ ревизија.

Во фазата на прелиминарните истражувања се применуваат методи кои не можат „механички да се следат или применуваат" како што се искуство, имагинација, креативност. Информациите можат да се соберат врз основа на физички докази, документи (вклучувајќи и писмени изјави), усни сведочења/ разговори, или со други средства во зависност од целите на ревизијата.

Со прелиминарното истражување се добиваат почетни податоци (сопствен изворен материјал) со помош на прашалници, искуства од претходни ревизии и директни

набљудувања. Исто така се користат и податоци/материјали кои произлегуваат од други субјекти или лица.

Како најчести извори на информации во субјектот предмет на ревизија, а кои се однесуваат на информациските системи, можеме да ги издвоиме:

- дијаграм на тек - дијаграм на тек на систем (system flow diagram), дијаграм на тек на податоци (data flow diagram), дијаграм на тек на процеси (process flow diagram), итн.;
- документи за системски развој од типот на Документ за спецификација на кориснички барања (User Requirement Specification Doc) , Спецификација на системски барања (System Requirement Specification);
- електронски податоци;
- други достапни информации во врска со функциите, контролата и мониторинг врз системите на субјектот, итн., како на пр. формулари/обрасци, буџетски информации, различни извештаи, вклучително извештаи од претходни ревизии, надворешни ревизии, внатрешни проверки, итн.;
- стратегии, политики, процедури и други упатства и
- корисниците на системот.

Сите податоци и информации треба грижливо да бидат собрани и документирани. Истите можат да послужат и како докази во подоцнежните фази од ревизијата.
Од особена важност е да се оцени веродостојноста на прибраните информации, односно дали тие даваат субјективна или објективна слика.
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.

3.1.1.4. Проценка на ризик во прелиминарното истражување

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.
Ревизорите треба активно да го контролираат ревизорскиот ризик[18], односно ризикот од неточни или нецелосни заклучоци, давање небалансирани информации или не обезбедување додадена вредност за корисниците.
Информациите до кои е дојдено со прелиминарното истражување, како и нивната анализа се основа за проценка на потенцијалните ризици кај конкретната ревизија на информациските системи.

Главната цел на проценатa на ризиците е да се добие уверување дека информацискиот систем ги штити средствата, овозможува интегритет на податоците, поттикнува ефективно остварување на целите на субјектот и ефикасно ги употребува ресурсите, односно контролите функционираат ефикасно и оневозможуваат да се случи грешка или неправилност.

Во зависност од влијанието на утврдените ризици во одделните области, зависи дали ќе се продолжи со извршувањето на ревизијата.
Ризиците и нивното влијание ќе бидат формулирани во соодветните области кои ќе дадат одговор на целта/целите на ревизијата, разработени преку соодветни ревизорски прашања.
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.

При прелиминарното истражување треба да се процени значајноста на ризиците, веројатноста за нивно настанување, како и можните последици. Ревизијата треба да се фокусира на ризиците кои имаат голема веројатност за настанување и чие влијание би било материјално или значајно, земајќи ги во предвид преземените мерки за минимизирање на овие ризици од страна на субјектот или инволвираните во одредена област согласно темата на ревизијата.
Проценката на ризиците од соодветна област е обработена во областите за ИТ ревизија и во прилозите на овој прирачник.

3.1.2. Ревизорски пристап и опфат

Општиот ревизорски пристап е централен елемент на секоја ревизија. Тој ја утврдува природата на проверката која треба да се направи. Исто така, ревизорскиот пристап ги дефинира потребното знаење, информации и податоци кои треба да се обезбедат и анализираат, како и ревизорските постапки кои треба да се спроведат.

[18] ISSAI 300/28

ИТ ревизијата вообичаено следи еден од трите пристапи:

- **системски-ориентиран пристап** - ревизорот е насочен кон проверка на функционирање на системите за управување, односно дали системите се воспоставени и истите правилно функционираат. Со овој пристап се дава одговор на прашањето: *„Дали, на кој начин и како се воспоставени и функционираат системите со кои е воспоставено управувањето со субјектите“?*
- **пристап ориентиран кон резултати** - ревизорот е насочен кон анализа и испитување на реализацијата на програмите, системите во однос на економичноста, ефикасноста, и ефективноста поврзувајќи ги со ревизорските критериуми. Во овој пристап наодите се дефинираат како отстапувања од поставените критериуми, правила и норми. Со овој пристап се дава одговор на прашањето: *„До каде е реализацијата на програмата, системот и дали целите се исполнети„?*
- **проблемски-ориентиран пристап** - со кој се проверуваат, потврдуваат и анализираат причините за одредени проблеми или отстапувања од утврдените критериуми, односно е насочен кон проблемите и се занимава со верификација и анализа на проблемите. Главна задача на ревизорот е преку независна анализа да ги утврди и констатира проблемите за одредена тема и да ги анализира нивните причинители. Со овој пристап се дава одговор на прашањето: *„Дали проблемите навистина постојат и кои се причините за нивното постоење?“*

Ревизорите треба да изберат пристап ориентиран кон резултати, проблеми или системи, или комбинација од истите за што подобро осмислување на ревизијата.[19] Сите три пристапи може да се применуваат од две различни перспективи: „одгоре - надолу” (top-down) или „оддолу - нагоре” (bottom-up). Ревизиите кои се вршат од перспектива „одгоре - надолу” се фокусираат главно на барањата, намерите, целите и очекувањата на законодавната и извршната власт. Пристапот од перспективата „оддолу – нагоре” се фокусира на проблеми од значење за поединецот и заедницата. Целта на ревизијата влијае врз тоа кој ревизорски пристап ќе биде избран. Исто така соодветни ревизорски техники се разликуваат во зависност од критериумите кои треба да бидат тестирани.

Од како ќе се одреди ревизорската цел, потребно е да се определи опфатот на ревизијата. Опфатот ја претставува рамката или ограничувањата на темата на ревизијата. Опфатот јасно одредува до кој степен ќе извршиме испитувања на клучните области / прашања. Со опфатот на ревизијата се осигурува дека фазата на испитување е јасно одредена, овозможува донесување на одлуки за потребните ресурси и ревизорските процедури кои треба да се преземат.

[19] ISSAI 300/26

3.1.3. Цел на ревизијата

Ревизорската цел треба да бидат поставена на почетокот на процесот на ИТ ревизијата за да помогне во утврдувањето на прашањата/задачите на ИТ ревизијата. Ревизорската цел и опфатот на ревизијата се меѓусебно поврзани и истите треба заедно да бидат разгледувани. Ефектите од поставената цел на ревизијата се протегаат низ секоја фаза на ревизијата. Тие го одредуваат пристапот и осмислувањето на ревизијата, опфатот, спроведувањето на ревизијата, временската рамка и природата на извештаите.

При поставувањето на целите, основен предуслов е солидно познавање на субјектот на ревизија и неговите информациски системи. Познавањето на субјектот подразбира познавање на деловните, финансиските и вообичаените ризици со кои се соочува ИТ системот на субјектот, како и самиот субјект. Дополнително, мапираните работни процеси на субјектот во неговото ИТ опкружување, како и степенот на ангажирање надворешни соработници и компании во реализирањето на работните процеси, се информации кои на ревизорскиот тим ќе му користат при утврдување на потенцијалните проблеми и опфатот на работата.

Ревизорската цел треба да биде поставени така што:
- ќе се даде одговор на значајните аспекти на ревизијата, (економичност, ефикасност и ефективност);
- ќе претставуваат области на кои може со ревизијата да се даде додадена вредност;
- ќе биде/бидат постигнати со ресурсите кои се на располагање.

Целта/целите по својата природа можат да бидат: нормативни и аналитички цели.

Нормативните цели – даваат одговор на прашањето: Дали работите се како што треба да бидат?. Нормативните цели претставуваат споредба на состојбата со конкретен критериум, закон, правилник и слично.

Аналитички цели на ревизијата даваат одговор на прашањето: Зошто работите не се како што треба да бидат?

Целта/целите на ревизијата се поставуваат во Предлогот на ревизијата на успешност и во Ревизорската програма.
Можни цели на овој вид ревизија се:
- 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.

3.1.4. Комуникација при планирањето на ИТ ревизијата

Ревизорите треба да одржуваат ефективна и соодветна комуникација[20] со субјектите на ревизија и останатите засегнати страни во текот на ревизијата. Ревизорите треба да ги идентификуваат одговорните лица и другите клучни засегнати страни, и да преземат иницијатива за воспоставување ефективна двонасочна комуникација. Преку добра комуникација, ревизорите може да го подобрат пристапот до изворите на информации, податоци и мислења од субјектот на ревизија.

3.1.4.1. Известување на субјектот за намера за вршење на ИТ ревизија

Ревизорите треба да ги известат субјектите на ревизија за клучните аспекти на предметот/темата на ИТ ревизијата.
Процесот на комуникација започнува со писмено известување (Прилог 11) за најава за почеток на ревизија кое се испраќа до субјектот предмет на ревизија. Известувањето треба да ги содржи следните информации:

- темата на ИТ ревизијата (област, активност, договор);
- ревизорскиот тим кој ќе ја врши ИТ ревизијата;
- период на извршување на ИТ ревизијата;
- потребна техничка поддршка на ИТ ревизијата и
- други информации и документација кои треба да ги обезбеди субјектот/субјектите предмет на ревизија.

3.1.4.2. Одржување на воведна средба (првичен состанок)

Ревизорскиот тим треба да организира и одржи воведна средба со раководството и одговорните лица на субјектот за почетокот на извршување на ИТ ревизијата. Првичен состанок има за цел да го запознае раководството со процесот на ИТ ревизија и да се воспостави позитивна комуникација. Првичниот состанок му дава можност на раководството и одговорните лица да постават прашања за ИТ ревизијата, како и да предложат аспекти на кои ќе треба да им се даде дополнително внимание.
Првичниот состанок треба да биде документиран во работна белешка.

3.1.4.3. Вршење ревизија кај други субјекти релевантни за ИТ ревизијата

Во текот на ИТ ревизијата, може да се јави потреба од вклучување на други субјекти. За потребата од вршењето на ИТ ревизијата кај други субјекти потребно е да се испрати известување (Прилог 12). Доколку во текот на ИТ ревизија има потреба од дополнителна документација се доставува Барање за документација (Прилог 13).

[20] ISSAI 300/29

3.1.4.4. Информирање на субјектот доколку ИТ ревизијата не продолжува

Доколку со прелиминарните истражувања ревизорскиот тим констатира дека нема да се продолжи со ИТ ревизијата истото го истакнува во Извештајот од прелиминарното истражување. За одлуката да не се продолжи со ревизијата се известуваат субјектот/субјектите на кои е најавена намерата за вршењето на ревизијата. (Прилог 14)

3.1.5. Извештај од прелиминарно истражување

Резултат од извршеното прелиминарно истражувања е изработката на **Извештај од прелиминарно истражување**[21] (Прилог 15), кој треба да содржи препорака за следната фаза, односно дали да се продолжи со ревизијата или истата да биде прекината со објаснување зошто е донесена таквата одлука.
Извештајот од прелиминарното истражување ги содржи следниве елементи:

- **Тема на ИТ ревизијата** - во овој дел се наведува темата предвидена во Годишната програма за работа на Државниот завод за ревизија.

- **Општи информации за областа предмет на истражување** - се опишува темата на ИТ ревизијата, податоци за информациските системи, снимените ИТ системи и апликации кои се поврзани со предметот или темата на ревизијата, законска и подзаконска регулатива која ја регулира темата.
- **Првични цели на прелиминарното истражување** - во овој дел треба да се наведат првичните цели и добиените информации од прелиминарното истражување. Првичните цели се утврдуваат преку детектирање и испитување на потенцијалните значајни ризици, дефинирање на проблемите произлезени од истражувањата.

- **Ревизорскиот пристап** - во овој дел потребно е да се наведат: ревизорскиот пристап и техниките на прибирање на податоци за ИТ ревизијата.

- **Опфат на прелиминарното истражување** - треба да се наведе периодот опфатен со ревизијата како и субјектите кои ќе бидат опфатени со ИТ ревизијата.

- **Предлог на значајни области** - ревизорите ги дефинираат и групираат областите според нивната значајност, а кои ќе бидат поместени и разработени во Ревизорската програма и ќе бидат предмет на понатамошни испитувања во фазата на извршување на ревизијата.

- **Утврдени ризици во прелиминарното истражување кои во понатамошниот тек на ревизијата можат да се покажат како значајни** - се наведуваат сите значајни ризици кои во прелиминарното истражување се првично утврдени и

[21] ISSAI 300/28,29, 33 и 37

анализирани и кои ќе овозможат соодветно планирање на активностите на ревизорите во натамошниот тек од ревизијата.

- **Заклучоци од прелиминарното истражување** - во овој дел ревизорите ги презентираат утврдените состојби од прелиминарното истражување. Во заклучоците потребно е да се наведат состојбите, критериумите од дадената област, причините за настанатите состојби и ефектот од истите. Вака дефинираните заклучоци треба да бидат поткрепени со достатни и соодветни ревизорски докази. Утврдените состојби и заклучоци во фазата на планирање не се конечни и истите можат да претрпат измена во понатамошните фази од извршувањето на ревизијата.

- **Препораки за продолжување или прекинување со ревизијата** - во зависност од резултатите од прелиминарните истражувања и прибраните документи и докази, тимот кој го извршил прелиминарното истражување предлага да се продолжи или не со извршувањето на ревизијата.
  Ако препораката се однесува на продолжување на ревизијата, треба да се даде објаснување за очекуваните ефекти од ревизијата.
  Доколку ревизорскиот тим предложи да не се продолжи со ревизијата потребно е да се образложат причините врз чија што основа е даден предлогот.

- **Потреба од користење на експерт** - доколку ревизорскиот тим утврди потреба од користење на експерти или други надворешни ресурси, потребно е истото да го образложи, и да ја утврди временската рамка, да даде информација за потребните финансиски средства, како и периодот за нивно ангажирање.
  Државниот завод за ревизија го регулира ангажирањето на експерти во ревизијата согласно соодветната законската регулатива на РМ.

Извештајот од прелиминарното истражување го изработува и потпишува ревизорскиот тим кој го спровел истражувањето и помошникот на главниот државен ревизор/раководителот на ревизија.

3.1.6. Предлог за ИТ ревизија

По одобрениот Извештај од прелиминарното истражување, ревизорскиот тим изработува Предлог[22] за ИТ ревизија (Прилог 16). Предлог за продолжување/не продолжување на ИТ ревизија се доставува со Писмо за предлог за продолжување – не продолжување на ревизија до Главниот државен ревизор (Прилог 17).
Основни елементи на предлогот за ИТ ревизија:

- **Тема на ревизијата;**
- **Утврдени области и значајни ризици;**
- **Заклучоци од прелиминарното истражувања;**

[22] ISSAI 300/37

- **Цел на ревизијата** и
- **Очекувани резултати од спроведувањето на ревизијата на успешност.**

Предлогот на ИТ ревизија го потпишува ревизорскиот тим и помошникот на главниот државен ревизор/раководителот на ревизијата, а се доставува на одобрување до главниот државен ревизор.

3.1.7. Ревизорска програма

3.1.7.1. Вовед

Ревизорската програма[23], во понатамошниот текст - Програма, (Прилог 18), во ревизијата на успешност ги дава главните насоки за постапување во фазата на извршување на ревизијата. Програмата ги содржи конкретните постапки и чекори, начинот на кој ќе се врши ревизијата и како ќе се прибираат ревизорските докази.

Програмата треба на јасен и концизен начин да ја дефинира целокупната работа во рамките на секоја одделно утврдена област и тоа: значајни ризици, дефинирање на прашања/задачи кои ќе бидат предмет на ревизија, критериумите, опфатот, техниките за прибирање и анализа на докази, утврдување на ограничувачките фактори при извршување на ревизијата како и очекуваните резултати.

Ревизорската програма претставува документ за:

- насоки за прибирање на докази во фазата на извршување на ревизијата;
- основа за документирање и обележување на ревизорската работа;
- рамка за распределба на задачите помеѓу членовите на ревизорскиот тим.

3.1.7.2. Изработка на Ревизорска програма

Програмата се изработува по завршувањето на прелиминарното истражување од кое ќе произлезе извештај од прелиминарно истражување.
При изработка на програмата од голема важност е ревизорите да ја имаат во предвид додадената вредност која се очекува од ревизијата.
Извештајот од прелиминарно истражување претставува влезен документ при изработка на програмата.
При изработката на програмата треба да се има во предвид и пристапот што ќе биде применет во конкретната ревизија.

3.1.7.3. Елементи на Ревизорската програма

Елементите на Програмата во Државниот завод за ревизија се следниве:

[23] ISSAI 300/37

- **Тема на ревизијата** - во овој дел се презентира темата на ревизијата планирана со Годишната програма на Државниот завод за ревизија.

- **Цел на ревизијата** - **о**вој дел ја содржи целта на ревизијата која е определена во Предлогот за ревизијата на успешност.

- **Области** - со цел да се олесни извршувањето на ревизијата и да се добијат помали фокусни делови препорачливо е утврдените значајни ризици, да се групирани по области, а секоја област може да се подели согласно клучните елементи од областа која е предмет на ИТ ревизија. Областите првично се утврдени во Извештајот од прелиминарното истражување. При изработка на Програмата првично утврдените области по потреба може да се намалат/зголемат, со цел да се постигне поголема ефикасност на ревизијата.
  Доколку во текот на ревизијата се утврдат области кои не биле утврдени со прелиминарното истражување и не биле планирани во ревизорската програма, потребно е да се изврши нејзина промена. Во одредена ИТ ревизија можно е да биде дефинирана само една област.
  Како можни области се ИТ управување, развој и набавка, ИТ операции, ангажирање надворешни соработници, план за деловен континуитет и план за обновување по катастрофа, информациска безбедност, апликациски контроли, дополнителни теми од интерес и други.

- **Ризици** - Значајните ризици утврдени со прелиминарните истражувања и презентирани во Извештајот од прелиминарно истражување, во Програмата се групираат согласно клучните елементи од областа која е предмет на ИТ ревизија. Во зависност од нивниот карактер се дефинираат и ревизорските прашања/задачи кои треба да се предмет на понатамошно испитување со помош на ревизорски техники. Утврдените ризици се потенцијални наоди уште во раната фаза на ревизијата, односно во прелиминарното истражување. Овие ризици во фазата на извршување на ревизијата треба да се продлабочат со понатамошни испитувања и анализи со цел да се постигнат очекуваните резултати или заклучоци.
  Доколку дополнително се утврдат значајни ризици, наоди кои не биле утврдени со прелиминарните истражувања и не биле предвидени во Програмата потребно е истата да се промени и дополни.

- **Прашања/задачи (колона 1)** - По дефинирање на областите и ризиците за секоја област одделно, потребно е да се дефинираат прашањата/задачите за ревизијата. Она што е особено важно при изработката на Програмата е прашањата/задачите да бидат јасно дефинирани. Треба да се избегнуваат двосмислени прашања. Поставувањето на прашањата вклучува објаснување на следново: што е она што сакаме да дознаеме?, кој е проблемот кој се истражува?, која е целта што треба да се постигне?. Прашањата треба да бидат дефинирани и насочени за да можат да

ја опфатат целта за секој поединечен ризик од областа. За еден утврден ризик можат да бидат поставени повеќе прашања/задачи.

Прашањата односно задачите потребно е:

- да се однесуваат на целта на ревизијата, утврдениот ризик и да овозможуваат собирање на релевантни докази кои ќе го зголемат ефектот на ревизијата;
- да се јасно поставени за да може ревизорите да ги разберат и прецизно да се насочат во ревизорските испитувања;
- да се подредени на логичен начин за ревизорското испитување да биде извршено на што е можно поефикасен начин;
- да се овозможи ефикасен начин на собирање на доволно докази без да се врши непотребно тестирање и да се трошат ревизорски ресурси.

Прашањата/задачите треба да бидат: јасни, конкретни, разумни, објективни, мерливи и возможни.

Воедни, овие прашања/задачи можат да бидат:

Описни прашања – преку овие прашања се осознава каква е и каква била состојбата.

Нормативни прашања – се утврдува разликата меѓу состојбата и критериумите. Во одредени случаи поставените прашања можат да содржат и критериуми (закон, стандарди, правилник, упатство, тарифник и слично) кој треба да се исполнат /почитуваат.

Причинско – последични прашања – ги испитуваат ефектите, размерот или големината на промените или разидувањата. Причинско – последичната анализа е вообичаен пристап кој се користи при евалуации и анализи.

Практични примери на прашања кои можат да послужат како дел на ревизорската програма за одредени области односно клучни елементи дадени се во Прилог 19 на овој прирачник.

- **Критериуми (колона 2)**

Ревизорите треба да воспостават критериуми[24] кои соодветствуваат на ревизорските прашања и се однесуваат на принципите на економичност, ефикасност и ефективност. Критериумите во ИТ ревизијата, претставуваат разумни и достижни стандарди со кои може да се оцени: економичноста, ефикасноста и ефективноста на системите.

При оформувањето на ревизорските наоди, критериумот служи за давање на одговор на прашањето - „*каква треба да биде состојбата или што треба да биде*?“.

За секоја ИТ ревизија треба да се определат општи и посебни критериуми. При определувањето на критериумите потребно е да се разговара со менаџментот или одговорните лица, за да се избегне ризикот од избор на погрешни критериуми.

[24] ISSAI 3000 Прилог 2; ISSAI 300/27

Критериумите можат да бидат: **општи и специфични**.

Општите критериуми најчесто се резултат на логично и рационално размислување. Овие критериуми треба поретко да се користат, а при тоа не треба да се употребуваат зборови кои упатуваат на неодредени општи критериуми како што се: соодветно, доволно, правилно, адекватно и слично, од причина што истите немаат исто значење.

Специфичните критериуми се тесно поврзани со конкретните активности и процеси на определена област од предметот на ревизијата како што се: законски прописи, стандарди, правилници, ценовници, тарифници, програми и слично. За оформување на критериуми од специјалистички или технички области ревизорите пожелно е да побараат помош од стручни лица или експерти од областа.
Постои широк спектар на извори за определување на критериуми и тоа:

- стратешки документи, законски и подзаконски акти;
- финансиски извештаи; буџети, финансиски планови и слично;
- програми и проекти;
- ревизорски критериуми оформени од други ВРИ;
- стандарди од домашни и меѓународни тела;
- владини политики и упатства;
- искуства на добра пракса;
- критериуми создадени од експерти;
- стручна литература; научни студии и истражувања;
- формални интервјуа од експерти;
- записници, одлуки на управни одбори и друго.

Карактеристики на добрите критериуми се веродостојност, објективност, корисност, разбирливост, споредливост, целосност, прифатливост[25].

- **Опфат (колона 3)**

Во рамките на Програмата потребно е да се утврди опфатот за секоја утврдена област и ризик. Опфатот[26] ја одредува рамката или границите на активностите кои треба да се преземат, субјектите кои ќе бидат предмет на ревизија и временскиот период кој ќе се опфати со ревизијата. Опфатот одредува до кој степен ќе вршиме испитување на клучните области/прашања.

При дефинирањето на опфатот на ревизијата потребно е да се имаат во предвид следните прашања:

- Кои ИТ системи и нивни функционалности ќе бидат предмет на испитување (сите, дел)?
- Кои активности од ИТ процесите ќе бидат предмет на испитување (сите, дел)?
- Кои ИТ контроли ќе бидат предмет на испитување (сите, дел)?

[25] ISSAI 3000, Прилог 2
[26] ISSAI 300/26

- Кои субјекти ќе бидат опфатени (сите, дел, во зависност дали се работи за ИТ систем кој е користен од еден субјект или повеќе)?
- Кој временскиот период ќе се испитува?
- Кои ќе бидат изворите на информациите за испитувањето, надворешни или внатрешни извори, кои може да имаат влијание на опфатот на ревизијата?
- Географски опфат на ревизијата (локации на ИТ системите).

- **Техники за прибирање и анализа на податоци/докази (колона 4)**

При изработката на Програмата од суштинско значење е техниките[27] за прибирање и анализа на податоци/докази да бидат внимателно избрани. За секоја дефинирана област, утврден ризик и поставени прашања/задачи, а со цел да се одговори на зададената цел и да *се добијат доволни докази* се избираат соодветни техники.
Техниките за прибирање на податоци треба да се засноваат врз проценка на ризик и ревизорските резултати кои се очекуваат да се добијат со избраните техники имајќи го превид расположливото време и ресурси за ревизијата.
При тоа можат да се користат една, две или комбинација од повеќе техники.
Во праксата постојат повеќе техники: проверка на документација; пребарување низ стручна литература; разговори/интервјуа; истражувања со прашалници; анализа на податоци; физичко набљудување/фотографирање; користење на експерти и фокусни групи и семинари и презентации.

Покрај претходно наведените техники, ревизорот може да користи и стандардните техники од ревизијата на успешност, како и техниките кои се содржани во поедините области за ИТ ревизија.

Вадење /издвојување/извлекување на 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/извлече податоци од копијата на податоците. Од ИТ 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 и апликациски системи

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

[27] ISSAI 3000, Прилог 1 точка 5

различните алатки (utilities) на компјутерските системи. Употребата на некоја од нив или нивна комбинација ќе зависи од целите и опфатот на ИТ ревизијата.

Тестирање на податоци

Тестирање на податоци може да се примени во ситуации кога е потребно тестирање на квалитетот на системот или апликацијата. Доколку истите се веродостојни за група специфични тестови може да се претпостави дека системот односно апликацијата се целосно веродостојни.

Оваа техника подразбира дизајнирање тест податоци и креирање тест податоци пред да се започне со употреба на програмата со тест податоци.

Специфични техники во ИТ ревизијата

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.

- **Ограничувачки фактори (колона 5)**

Во Програмата ревизорите потребно е да ги идентификуваат можните проблеми и ограничувачките фактори. Главни поставувани прашања и проблеми кои треба да се обработат во овој дел се: кои се предупредувањата, одредувањето на квалитетот и веродостојноста на податоците, дали има ограничување на пристап при вршењето на ревизијата, дали ревизорите имаат ограничени ресурси: технички ресурси, ограничување за патување, има ли значителни ограничувања за пристап до информации и до официјални лица, односно кои се можните ограничувачки фактори при извршување на ревизијата.

- **Очекувани резултати (колона 6)**

При изработка на Програмата потребно е ревизорите да ги предвидат очекуваните резултати. Резултатите од ревизијата претставуваат индикатори за следење на програмата и се користат за мерење на ефектот од ревизијата. При предвидувањето на резултатите од ревизијата потребно е ревизорите да посветат внимание на прашањето: што се очекува да се најде/открие и/или со какви подобрувања (економичност, ефективност и ефикасност) ќе придонесе ревизијата? Да се направи листа на можни / потенцијалните состојби/ очекувани резултати, во врска со предметот на ревизијата. Очекуваните резултати најчесто даваат одговор на ревизорските прашања/задачи, односно даваат одговор на прашањето што е она што сакаме да го дознаеме.

- **Одобрување на ревизорската програма**[28]

Ревизорската програма ја изработува ревизорскиот тим, а ја одобрува ПГДР/РР.

Во Прилог 19 на овој прирачник изработен е пример за ревизорска програма.

- **Измена и дополнување на ревизорската програма**

Како што ревизорите подобро се запознаваат со темата на ревизија, често се случува првично утврдените ризици и донесените заклучоци во раните фази од ревизијата да има потреба да се преиспитаат. Од тие причини ревизорите треба да бидат флексибилни и да бидат подготвени да го прилагодат својот пристап на сите нови информации.
Измената и дополнувањата на ревизорската програма е детално објаснета во фазата на извршување на ревизијата во точката Измена и дополнување на ревизорската програма.

3.1.8. План на активности со временска рамка за реализација на ИТ ревизијата

За успешно извршување на севкупната ревизија потребно е да се изработи детален План на активности со временска рамка за реализација на ИТ ревизијата по области/ризици. Во овој документ потребно е да се одредат: временските рокови, ревизорите, задачите кои ќе ги извршуваат како и евентуалното користење на експерти или други надворешни лица.
Деталната временска рамка за севкупната ревизија треба да биде опфатена во посебен документ – План на активности со временска рамка за реализација на ИТ ревизијата. (Прилог 20) .

[28] ISSAI 40/3

3.2. Извршување

Фазата на извршување на ревизијата започнува по одобрување на Ревизорската програма, а со цел остварување на поставените задачи и формирање заклучоци за степенот на економичноста, ефикасноста и ефективноста на активностите во областа предмет на ревизија.
Извршувањето вклучува повеќе ревизорски постапки: собирање и анализирање податоци, оценување факти со претходно утврдени критериуми, изготвување на првични заклучоци / ревизорски наоди и документирање на доказите.
Во фазата на извршување од суштинско значење за ревизорите е професионалното расудување и непристрасен став кон информациите и аргументите како и проценка на квантитетот и квалитетот на доказите кои ќе овозможат донесување на правилни заклучоци во врска со ревизорските прашања и одредување на значењето на утврдените состојби. Генерално организирањето на ревизијата, треба да ги задоволи барањата за добро управување со ревизијата.
Во фазата на извршување на ревизијата работата на ревизорите како и документацијата од извршената работа треба да биде надгледувана од страна на одговорни лица.

3.2.1. Ревизорски докази

3.2.1.1. Вовед

За извршување на ревизијата неопходно е да се обезбедат компетентни, релевантни и разумни докази како поткрепа на ревизорските просудувања и заклучоци кои се однесуваат на субјектот/субјектите, информациските системи апликациите и активностите кои се предмет на ревизија.
Стандардите на ISSAI исто така пропишуваат дека ревизорските наоди, заклучоци и препораки мора да се засноваат на докази. Бидејќи ревизорите ретко имаат можност да ги разгледаат сите податоци кои се однесуваат на субјектот/областа која е предмет на ревизија, од голема важност е прибирањето на податоци и техниките за тестирање со примерок внимателно да се изберат. Со оглед на тоа дека компјутерски базираните системи на податоци се важен дел од ревизијата, а сигурноста на податоците е битна за остварување на целите на ревизиите, ревизорите ќе треба да се уверат во сигурноста и релевантноста на податоците.
Доказите претставуваат информации кои се собираат и потоа користат како база на факти врз основа на која се снима ситуацијата и се донесуваат заклучоци во рамки на поставените ревизорски цели. Доказите се основа врз која го градиме нашето уверување дека нешто е вистинито или не е, со тоа што даваат убедлива поткрепа за некој факт или одговор на некое прашање. Доказот ја поткрепува содржината на ревизорскиот наод, вклучително и описниот материјал како и сите снимени состојби и заклучоци од кои произлегуваат препораките.

3.2.1.2. Природа на доказите

Податоците, информациите и ревизорските докази се меѓусебно поврзани, и тоа:

Природата на доказите варира, со тенденција доказот да биде убедлив. Природата на ревизорските докази е одредена исклучиво од предметот на ревизијата и ревизорските прашања кои се разликуваат од една до друга ревизија и е резултат на расудување на ревизорот. Некои ревизорски докази се сметаат за поубедливи, а други се убедливи според својата природа, но истите во голема мера зависат од креативноста на ревизорите. Деталните проценки за потребите од информации треба да се вршат уште во фазата на планирање со цел ревизорите да избегнат да бидат преплавени со прекумерни податоци. Ревизорите треба секогаш да се обидуваат да бидат практични во своите напори да прибираат и анализираат податоци за кои сметаат дека ќе им бидат најпотребни.
Исто така би било корисно да се разговара однапред со експерти во врска со природата на податоците кои се добиени и начинот на кој тие ќе бидат анализирани и интерпретирани од страна на ревизорот, со цел да се намали ризикот од недоразбирање.

3.2.1.3. Видови на докази

Ревизорските докази се организираат во четири вида на докази:

- Физички - најубедлив доказ, за кој ревизорот мора да биде свесен дека неговото присуство може да има влијание врз квалитетот на доказите.
- Документарен - електронски формат или хард-копија. Корисните информации не можат секогаш да бидат документирани, затоа е неопходна употреба на други методи.
- Устен - усните докази се генерално од важност во ревизиите на успешност, меѓутоа истите треба да се потврдат со изјави доколку се користат како доказ.

Аналитички доказ кој се добива со користење на професионално расудување за да се оценат физичките, документарните и усните докази.

Видови на докази		Ревизорски постапки за добивање докази	Документација
Физички	Најубедлив доказ, за кој ревизорот мора да биде свесен дека неговото присуство може да има влијание врз квалитетот на доказите.	Непосреден увид или набљудување на луѓе, имот или настани	Белешки, фотографии, графикони, мапи, цртежи, примероци или аудио-визуелни материјали.
Документарен	Електронски формат или хард-копија. Корисните информации не можат секогаш да бидат документирани, затоа е неопходна употреба на други методи.	Преглед на документи, извештаи, прирачници, весници, интернет, поштенски или веб-базирани анкети.	Извештаи, политики и процедури, писма, договори, резултати од истражувањето.
Устен	Усните докази се генерално од важност во ревизиите на успешност. Истите треба да се потврдат со изјави доколку тие се користат како доказ.	Прашања или интервјуа на ревидираниот субјект на вработените или трети лица, фокус групи, експертски панели.	Резиме на информациите добиени преку овие методи.
Аналитички	Доказ кој се добива со користење на професионално расудување за да се оценат физичките, документарните и усните докази.	Анализа преку размислување, рекласификација, пресметка и споредба.	Резиме на аналитички податоци, вклучувајќи анализа за сооднос, регресивна и компаративна анализа.

3.2.1.4. Извори на докази

Постојат три вида извори на докази во ИТ ревизиите и истите се обезбедуваат на следниот начин:

- Генерирани директно од страна на ревизорите - Интервјуа, анкети прашалници, фокус групи, непосреден увид и физичко набљудување. Ревизорите можат да утврдат - техники со кои ќе се обезбеди најдобар квалитет на докази за конкретната ревизија. Од нивните вештини во дизајнирање и примена на методи ќе се утврди квалитетот на доказите.
- Обезбедени од страна на субјектот - Информации од базите на податоци, документи, изјави, активности датотеки. Треба да се утврди веродостојноста на податоците кои се значајни за ревизорските прашања преку разгледување и потврдување, тестирање на интерните контроли на субјектот и општи и апликативни контроли преку компјутерски обработени податоци.

- Обезбедени од трети страни - Докази потврдени од други страни, чиј квалитет е добро познат (статистички податоци).

Степенот до кој информациите можат да се користат како ревизорски докази зависи од степенот до кој може да се утврди неговото значење за квалитет на ревизорските наоди.

3.2.1.5. Карактеристики на доказите на ревизијата

Релевантноста, доволноста и веродостојноста на доказите се три основни карактеристики на доказите.
Доволноста е квантитативен аспект на ревизорскиот доказ, а релевантноста и веродостојноста се аспект на квалитетот.
Ревизорите треба да бидат свесни за можните проблеми или слабости на доказите во ревизијата.
Доволни, релевантни и сигурни докази ревизорот треба да обезбеди за да добие поддршка на наодите и заклучоците на ревизијата.

3.2.1.6. Критериуми за доволност, релевантност и веродостојност на доказите

Во оценувањето на квантитетот и квалитетот на ревизорските докази, ревизорот треба да ги има во предвид следниве аспекти:

- **намената** за која ќе се користат доказите - ревизорските наоди треба да бидат поткрепени со доволни, релевантни и сигурни докази;
- степен на **материјалност** во монетарна смисла или **значајност** на ревизорскиот наод - за повисоко ниво на материјалност или значајност, потребен е „повисок степен" на докази;
- степенот на **независност** на изворот на доказите - поголема сигурност за докази кои произлегуваат од независни извори;
- **трошоците** за добивање дополнителни докази во однос на можната корист во смисла на поддршка на наоди и заклучоци - трошоците за добивање на повеќе докази не треба да ја надминат корисноста на доказите;
- **ризик** од формирање на неточни наоди и заклучоци - „повисок степен" на докази преку проширување на тестирањето и
- **внимание** за собирање и анализа на податоците - подобрување на вештините на ревизорите по области

Ревизорот мора да се увери дека квантитетот и квалитетот на доказите го минимизираат ризикот од невалидни или несоодветни наоди, заклучоци и препораки. Ако процесот на собирање докази не произведува доволни, релевантни и веродостојни докази, тогаш наодите и заклучоците кои произлегуваат од доказите, не треба да се обелоденат.

3.2.2.Методологија во фазата на извршување

ИТ ревизиите може да се извршуваат врз основа на различни методи и техники за собирање на податоци и техники за анализа на истите. Информациите и податоците

се собираат за да се разбере и опише предметот на ревизија, да се оцени и измери резултатот, да се откријат недостатоците, да се опишат и анализираат односите меѓу причините и последиците, да се провери претпоставката, да се објасни успешноста и да се проверат аргументите и предлозите. Анализата на податоците од хронолошки аспект следи по процесот на собирање на податоци.
Собирањето на докази во фазата на извршување се однесува на податоци и информации кои се подетални, за разлика од прелиминарното истражување, кога ревизорот е заинтересиран за добивање повеќе општи информации и податоци.
Не е возможно да се опишат сите техники на собирање и анализа на податоци кои треба да се користат. Некои од нив имаат за цел да овозможат познавања и добро разбирање, додека пак други се користат за верифицирање и селекција на основни факти.
Методологијата за ИТ ревизија детално е објаснета во секоја област од ИТ ревизијата.

3.2.3. Валидност (веродостојност) на ревизорските наоди

Анализата на податоците го води ревизорот до изведување/формулирање на наодите. Потребно е да се има јасна слика за ревизорските наоди кои треба да се дел од ревизорскиот извештај, како и нивните причини, критериуми и односи.
Основа за утврдување на ревизорските наоди, како и донесување на заклучоци и давање на препораки, се утврдените критериуми. Критериумите во ИТ ревизијата се стандард според кои нешто може да биде оценето. Ревизорските критериуми претставуваат збир на разумни и остварливи „стандарди на успешност“. Доколку нема поставено соодветни критериуми тогаш нема да има ни основа за споредба односно основа за утврдување на ревизорски наоди, донесување на заклучоци и давање на препораки. Критериумот уште од почеток треба да ни даде јасна слика што треба да бараме во текот на ревизијата.
За секоја ИТ ревизија треба да се определат општи и посебни критериуми. При определувањето на критериумите потребно е да се разговара со менаџментот или одговорните лица, за да се избегне ризикот од избор на погрешни критериуми.
Ревизорските критериуми можат да бидат изведени од бројни извори, а просудувањето на ревизорот игра важна улога во утврдувањето на релевантни и прифатливи извори на критериуми како што се: основни документи за планирање, физибилити студии и одобрени планови, финансиски извештаи на субјектот, извештаи за буџетот, извештаи за проекти, стандарди поставени од други меѓународни тела, владини политики и упатства, закони, правила и прописи, критериуми поставени од страна на раководството.
Во фазата на извршување постои потреба од собирање на дополнителни докази од ревидираниот субјект кое може да биде потребно за:

- да се утврди дали одредениот недостаток е изолиран пример или претставува систематски проблем;
- да се идентификува причината за недоволно обезбедени докази;
- да се утврди дали проблемот може да се реши од страна на субјектот или е надвор од негова контрола и да се оцени неговиот потенцијален ефект.

Во едни случаи, ефектот на наодот може да биде квантитативно голем, а во други случаи квалитативните ефекти на наодот можат да бидат значајни, при што истите треба да бидат предмет на конструктивна дискусија со ревидираниот субјект, кои на ревизорот ќе му бидат основа за формирање на првичниот наод.

3.2.4. Анализа за ревизорски наод

На крајот на фазата на извршување на ревизијата се врши анализа на доказите со која се утврдува основот на елементите на ревизорскиот наод: критериумот, состојбата, причината и ефектот. Целта на оваа анализа е да се извлечат првични заклучоци како основ за формирање на ревизорскиот наод. Заклучоците и наодите како резултат на анализата, треба да дадат одговор на ревизорските прашања.
Наодите констатирани во текот на извршување на ревизијата треба да бидат поставени во јасна и логична рамка за да се овозможи лесно разбирање на ревизорските критериуми кои се применуваат, идентификувани факти, како и анализа од страна на ревизорот за природата, значењето и причините на проблемот.
Во поглед на влијанието на наодот, мора да се има во предвид -економичноста, ефикасноста и/или ефективноста на употребата на информатичката технологија и ИТ системите, бидејќи тоа дава основ да се преземат корективни активности.
Ревизорот мора да го процени степенот на доверба во ревизорскиот наод, врз основа на валидноста на доказите. Проценката треба да се гледа јасно во текстот на наодот, со користење на соодветни квалификации.
ИТ ревизијата треба да се фокусира на обезбедување балансиран поглед на темата, презентирајќи не само недостатоци, туку и позитивни наоди и индикации за добра практика. Севкупниот акцент е да се формулира ревизорски наод на конструктивен и урамнотежен начин.
Понатаму, ревизорот треба да ја утврди свесноста на раководството на ревидираниот субјект за утврдените состојби. Доколку субјектот е свесен за утврдените состојби и веќе се преземаат корективни активности, тие треба да се евидентираат и да бидат земени во предвид при известувањето.

3.2.5. Измена и дополнување на ревизорската програма

Во фазата на извршување на ревизијата може да се утврдат промени кои влијаат на севкупното ревизорско работење, односно потреба од промена на ревизорскиот пристап, утврдени нови ризици, промена на опфатот на ревизијата, оправдани ограничувачки фактори за извршувањето на ревизијата, ангажирање на експерти, поради што е потребно да се изврши измена и дополна на Ревизорската програма.
За извршената измена и дополнување на Ревизорската програма потребно е ревизорите да изготват соодветно образложение во кое ќе се наведат потребата и причините од измена и дополна на Ревизорската програма.

3.2.6. Комуникација во извршувањето

Ревизорите треба да одржуваат ефективна и соодветна комуникација со субјектите на ревизија и останатите засегнати страни во текот на ревизијата.
Навременото пренесување на првично констатираните состојби/наоди или препораки на одговорните раководни лица на субјектот е важна ревизорска постапка, која помага при потврдувањето на првичните заклучоци / наоди во фаза на извршување на ревизијата и го поттикнува субјектот да даде свое мислење. Користа/ефектот од ИТ ревизијата ќе биде поголем од причина што ваквата постапка овозможува субјектот веднаш да преземе корективни мерки во проблематичната област.
На крајот од фазата на извршување на ревизијата треба да се одржи завршен состанок со одговорните раководни лица од субјектот. Целта на овој состанок е:

- да се презентираат најзначајните ревизорски заклучоци / наоди и препораки - презентација (Power Point Presentation), усно презентирање и други техники;
- да се разговара со раководството на субјектот за презентираните ревизорски наоди и препораки и да се добијат нивните коментари и
- да се даде можност на субјектот да ги разјасни недоразбирањата и да дискутира за ревизорските наоди и препораки.

Завршниот состанок треба да биде документиран и внесен во работните белешки. (Прилог 21 - Записник од завршен состанок).

3.2.7. Документирање на ревизијата

Ревизорите треба адекватно да ги документираат ревизорските докази во работни белешки, вклучувајќи ја и основата и обемот на планирањето, работата која е извршена и наодите од ревизијата.
Соодветната документација обезбедува:

- зголемување на ефикасноста и ефективноста на ревизијата;
- доказ за ревизорската усогласеност со ревизорските стандарди, правила, политики и процедури;
- олеснување на планирањето на ревизијата;
- извор на информации за подготовка на извештаи и одговор на било какви прашања од страна на ревидираната институција или од било која друга страна;
- извршување на делегирани задачи на задоволителен начин;
- обезбедување евиденција за слабостите, грешките и откриените неправилности од страна на ревизијата;
- потврда и поддршка на ревизорските мислења и извештаи;
- олеснување на надзорот и обезбедување на квалитет на ревизијата;
- помагање на професионалниот развој на ревизорот и
- обезбедување докази за извршената работа за идна употреба.

Документацијата треба да биде доволна и детална за да обезбеди разбирање на ревизијата.

3.2.7.1. Работни белешки

Работните белешки треба да содржат докази за поддршка на мислењата, заклучоците и анализите кои ги поддржуваат препораките во извештајот, помагаат при организацијата на ревизијата и го олеснуваат пристапот до доказната документација.
Работните белешки треба да бидат јасни, читливи, комплетни, релевантни, точни, концизни, уредни, и разбирливи и да се држат до прашањата кои се тесно врзани со целите на задачата. (Прилог 22 - Работна белешка).
Секоја работна белешка треба да ги содржи следните идентификациски информации: тема на ИТ ревизијата, име на субјектот каде е вршена ревизијата, соодветно да биде обележана, информации за лицето кое ја подготвило белешката, информација за датумот на изготвување на работната белешка, информација за лицето кое ја одобрило белешката и датумот на одобрување.
Во работната белешка треба да е наведен изворот на информацијата која ја содржи како и лицето/субјектот кое ја обезбедило информацијата. Секоја работна белешка треба да содржи цел, ревизорска област/ризик и прашање, со која ги објаснува причините за развивање и анализирање на информациите и користењето на информациите во однос на целта на ревизијата.
Работна белешка во која се содржани резултати од извршени анализи и проценка на информациите, односно работната белешка како заокружена целина, треба да има заклучок кој концизно и јасно ги објаснува резултатите на анализата на ревизорот и проценката на информациите.

3.2.7.2. Бележење на работните белешки

Бележењето е начин да се идентификува секоја работна белешка, односно претставува постапка за евидентирање на ознаките во работната белешка за да се идентификуваат информации кои се содржани во други работни белешки, а се надоврзуваат или се поврзани со дадена белешка. Секоја работна белешка треба да има единствена ознака/индекс/број согласно фазата на ревизија.
Потребно е да се врши вкрстено поврзување со сите други работни белешки кои се сметаат за битни во спроведувањето на соодветната анализа, преглед и толкување на резултатите содржани во конкретните работни белешки.

3.2.7.3. Организирање на ревизорски документи

Организирањето на ревизорските документи (работните белешки и друга прилог документација) се врши согласно Организациска шема на одлагање на ревизорски документи (Прилог 23).

Во истата е дадена организација на работните белешки идентификувани по конкретни групи - секции како и по видот на документација/поткрепа содржана во секоја од секциите.
Примената на Организациска шема на одлагање на ревизорски документи го олеснува пристапот до доказната документација, овозможува ефикасно управување на ревизиите, помага при проверката за осигурување на квалитет на ревизорската работа како и резултатите од извршената работа за поддршка на ревизорското мислење.

3.3. ИЗВЕСТУВАЊЕ

Известувањето кај ИТ ревизијата има за цел презентирање на резултатите од ревизијата кои ќе придонесат кон подобрување на состојбите во употребата на информатичката технологија и информациските системи во субјектите предмет на ревизија.

При вршење на ИТ ревизија како дел од ревизија на регуларност, ревизорскиот пристап треба да се заснова на ризик. Ревизорот треба да го планира и развива пристапот на ревизија со цел да се донесе заклучок за ефективноста на контролите врз процесите на информатичката технологија (ИТ процесите) што имаат директно влијание врз обработката на финансиските податоци.

Известувањето при вршење на ИТ ревизија како дел од ревизија на регуларност е согласно утврдената методологија на Државниот завод за ревизија и форматот на ревизорски извештај за ревизија на регуларност, со тоа што во делот на внатрешни контроли ревизорот ќе информира за ризиците во процесите кои се потпираат, односно користат информатичка технологија. Исто така ревизорот ја евалуира ефективноста на дизајнот на секој од главните процеси кои се потпираат на информатичка технологија и поврзаните внатрешни контроли. Доколку отстапувањето во контролите предизвикало грешки кои се материјални за финансиските извештаи, за утврдените состојби ревизорот ќе извести во соодветните делови од ревизорскиот извештај (Прилог 24 - ИТ ревизија како дел од ревизија на регуларност).

Кога ИТ ревизијата е главен фокус на ревизијата, станува збор за ревизија на успешност. Целта на ревизијата во овој случај е проучување на развојот на ИТ системите во субјектот предмет на ревизија и дали истите се усогласени со поставените ИТ стандарди. Ефикасноста на ИТ системите е важен аспект на капацитетот на системот што води до ефективно користење на ресурсите. Затоа субјектот на ревизија треба да усвои методологија/стратегија која ќе овозможи имплементација на системи со користење на техника дизајнирана да обезбеди ефективни системи без неприфатливи ризици кои би го загрозиле работењето на субјектот. Субјектот треба да го следи развојот на ИТ системот за да го спречи зголемувањето на трошоците кај системи кои не функционираат како што треба.

Добро планирана и спроведена ИТ ревизија претставува основа за добар извештај. Ревизорскиот извештај е конечен производ на ревизорскиот процес. За време на фазата на известување, ревизорот врз основа на заклучоци изготвува извештај со цел да даде одговор на поставената цел на ревизија, дефинирајќи ги наодите, заклучокот и препораките. Известувањето треба да биде согласно утврдената методологија на Државниот завод за ревизија и форматот на ревизорски извештај за ревизија на успешност. (Прилог 25- ИТ ревизија како ревизија на успешност)

3.3.1. Карактеристики на извештај

Ревизорски извештај кој придонесува за подобрување на економичноста, ефикасноста и ефективноста во користењето на средствата на граѓаните е одраз на

кредибилитетот и репутацијата на Државниот завод за ревизија. Добриот извештај треба да ги презентира главните наоди и заклучоци на ревизорските прашања, овозможувајќи му на читателот да разбере зошто и како ревизијата била спроведена и да понуди практични препораки кои ќе овозможат реални промени во управувањето со употребата на информатичката технологија и информациски системи.

Секој кој е вклучен во фазата на известување треба да ги има во предвид карактеристиките што треба да ги има еден ревизорски извештај за да препознаеме квалитетно известување:

Објективен - Ревизорскиот извештај треба да биде независен и објективен, да нема конфликт на интереси со ревидираните субјекти што би создало сомневање во неговата објективност и би го нарушил кредибилитетот на ревизорот и Државниот завод за ревизија во целина.

Сеопфатен - Извештајот треба да ги содржи сите информации и аргументи кои се неопходни за одговор на ревизорските прашања за да осигури дека заклучоците и препораките можат да се разберат.

Точен – Извештајот треба да се темели на доволни и релевантни докази. Методологијата и ревизорските постапки треба да бидат прикажани на јасен начин за да се елиминираат сомневањата во веродостојноста на извештајот како целина.

Концизен - Извештајот треба да ги покрива само релевантните аспекти за остварување на поставената цел на ревизијата, без вклучување на неважни информации.

Навремен - Извештајот треба да се изработи веднаш по завршување на ревизијата, за да биде корисен за оние за кои е упатен.

Јасен - Извештајот треба да биде лесен за читање и разбирање со јасно пренесена порака. Логичната структура на извештајот, точност во презентирање на фактите и конципирање на заклучоците е основа за јасен извештај и негово разбирање. Употреба на наслови и поглавја дава леснотија при читање и разбирање на извештајот. Илустративните алатки (слики, графикони и мапи) може да се користат за појасно презентирање на комплексна материја.

3.3.2. Форма и содржина на ревизорски извештај од спроведена ИТ ревизија

Извештајот треба да ја следи стандардната структура на формат за ревизија на успешност, која ќе му овозможи на читателот да се убеди во валидноста на наодите, разумноста на заклучоците и придобивките од имплементација на препораките. **Посебноста на ИТ ревизијата е во утврдената цел и опфат на ревизија.** Ревизорот треба да обезбеди уверување дека ИТ ресурсите овозможуваат ефективно постигнување на целите на субјектот и ефикасно искористување на ресурсите. ИТ ревизиите може да ги опфатат системите за планирање на ресурсите на субјектот предмет на ревизија, безбедноста на информациските системи, развојот на системите и нивното усогласување со ИТ стандардите.

Формата и структурата на извештајот е согласно методологијата за ревизија на успешност и ги содржи следните поглавја:

1. Резиме;
2. Основни податоци;
3. Цел, опфат и методологија на ревизијата;
4. Ревизорски наоди;
5. Заклучоци и
6. Препораки.

Ревизорскиот извештај може да содржи и прилози:

- Табели, графикони, фотографии, анализи и друго;
- Забелешки/коментари/известување на Нацрт извештајот;
- Одговор на забелешки/коментари/известување на Нацрт извештајот на Овластениот државен ревизор.

Прилог 26 – Ревизорски извештај

3.3.3. Одобрување и доставување на извештај

Согласно утврдената методологија на Државниот завод за ревизија изготвениот Нацрт извештај од страна на ревизорскиот тим се прегледува од страна на раководителот на ревизорскиот тим, по што се доставува до ПГДР/РР (согласно Упатството за контрола на квалитет на ревизиите).

Со цел оцена и утврдување на компактноста и квалитетот на Нацрт извештајот истиот се доставува до Стручното тело пред доставување на законски утврдените субјекти.

Нацрт извештајот се доставува со писмо (Прилог 27) до субјектите опфатени со ревизијата со можност за доставување на забелешки во однос на ревизорските наоди, заклучоци и препораки. Забелешките и соодветните образложенија од субјектите се анализираат од страна на ревизорскиот тим и Стручното тело.

Анализата и одговорот на забелешки се документираат во работни белешки. Забелешките и одговорот на забелешките (Прилог 28) се составен дел на Конечниот извештај.

Конечниот извештај се доставува со писмо (Прилог 29) до субјектите опфатени со ревизијата, извршната и законодавната власт.

Со Конечниот извештај се доставува образец Известување за преземени мерки по препораките на овластениот државен ревизор содржани во конечниот ревизорски извештај – ИЗПМ согласно Прирачникот за следење на препораките.

Во согласност со законската регулатива а со цел транспарентност во работењето сите извештаи се достапни за пошироката јавност на официјалната веб страна на Државниот завод за ревизија.

4. 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.

Резултатите од следењето на препораките од ревизијата треба да се евидентираат. Информациите за недостатоците и подобрувањата кои се откриени при спроведување на препораките, ако е потребно, треба да се достават до Владата или законодавецот[29].

Начин на следење на препораките

Согласно регулативата, Државниот завод за ревизија и кај овој вид ревизија го следи спроведувањето на дадените препораки 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,

[29] ISSAI 3000/5.4

- 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.

Одлуката за наведените алтернативи треба да биде дел на проценка согласно стратешките акти за ревизија на ВРИ[30], а содржано во Годишната програма за работа на Државниот завод за ревизија. Доволно време треба да им биде дадено на субјектите опфатени со ревизијата со цел имплементација на препораките.

[30] ISSAI 3100/36

5. КОНТРОЛА НА КВАЛИТЕТ И ОСИГУРУВАЊЕ НА КВАЛИТЕТ

5.1. 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.

ISSAI 40 – Контрола на квалитетот на ревизиите обезбедува насоки за врховните ревизорски институции за примена на основните принципи на контрола на квалитет, соодветно на нивниот мандат и околности. Овој стандард ги опишува основните мерки за остварување на ефикасна контрола на квалитет.

Насоките за контрола на квалитетот на ниво на поединечна ревизија на успешност се утврдени во:

- ISSAI 3000 Прилог 4 (во кои се дадени активностите на ВРИ за обезбедување квалитет) и
- ISSAI 300/32 (во кои се дадени насоки за контрола на квалитетот во ревизијата на успешност);

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

Согласно Упатството за контрола на квалитет на ревизиите, контролата на квалитет ги опфаќа сите фази на ревизијата на успешност: планирање со прелиминарни истражувања, извршување, известување и следење на препораките од ревизијата. За секоја од поединечните фази на ревизијата се дадени соодветни насоки за спроведување на контролата и обрасци – прашалници за оцена и контрола на квалитет. Исто така, со Упатството се утврдени и обврските на ревизорите, раководителот на ревизорскиот тим и раководителот на ревизијата/ПГДР за спроведување на контрола на квалитет на ревизијата .
За разбирање на концептот на контрола на квалитетот на ревизијата, значајно е да се потенцира дека тој е вграден во целиот процес на ревизијата, со конкретни постапки за обезбедување и потврдување на спроведените контроли на квалитет.
Во контролата на квалитет на ревизијата се инволвирани сите вработени задолжени за нејзино спроведување, согласно нивните надлежности.

5.2. Осигурување на квалитет

Осигурувањето на квалитет на ревизија на успешност може да се дефинира како процес преку кој ВРИ го проценува системот на контрола на квалитет (дали ефективно функционира). Осигурувањето на квалитет го извршува независен тим на искусни ревизори, кои не учествувале во конкретната ревизија.

Осигурувањето на квалитет на ревизии на успешност вклучува преглед на примероци на завршени ревизии (cold review), или на соодветни фази во текот на ревизијата (hot review). Цел на овие прегледи е да се осигура дека ревизиите се планирани и извршени во согласност со методолошките акти на Државниот завод за ревизија и да се увери дека се дадени мислења/заклучоци врз основа на достатни и соодветни докази. Исто така, со осигурување на квалитет на ревизиите ревизорскиот тим за осигурување на квалитет на ревизиите, сака да се увери дека сите поважни претпоставки донесени за време на фазата на планирање со прелиминарни истражувања, извршување и известување на ревизиите се содржани во работната документација.

ВРИ треба да усвои политики и процедури за проверка на ефикасноста и ефективноста на интерните контроли и процедури на ВРИ. (ISSAI 3100/38).

Секоја ВРИ треба да воспостави сопствен систем на процедури кои:

- Потврдуваат дека интегралните процеси на осигурување на квалитет работеле/функционирале на задоволително ниво;
- Обезбедуваат квалитет на ревизорските извештаи и
- Осигуруваат подобрувања и избегнување на повторувања на слабостите. (ISSAI 3000/прилог 4) .

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.

6. 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 – Примери за Дополнителни теми од интерес

Прилог 11 – Писмено известување за најава за почеток на ревизија.

Прилог 12 – Писмено известување кај други субјекти.

Прилог 13 – Барање за документација

Прилог 14 – Информирање на субјектот доколку ИТ ревизијата не продолжува

Прилог 15 – Извештај од прелиминарно истражување

Прилог 16 – Предлог за ИТ ревизија

Прилог 17 - Писмо за предлог за продолжување – не продолжување на ревизија до Главниот државен ревизор

Прилог 18 – Ревизорска програма

Прилог 19 – Практични примери за ревизорска програма

Прилог 20 - План на активности со временска рамка за реализација на ИТ ревизијата.

Прилог 21 - Записник од завршен состанок

Прилог 22 - Работна белешка

Прилог 23 – Организациска шема на одлагање на ревизорски документи

Прилог 24 - ИТ ревизија како дел од ревизија на регуларност

Прилог 25- ИТ ревизија како ревизија на успешност

Прилог 26 – Ревизорски извештај

Прилог 27 – Писмо за доставување нацрт-извештај

Прилог 28 – Одговор на забелешки

Прилог 29 – Писмо за доставување Конечен извештај