МИНИСТЕРСТВО ЗА ФИНАНСИИ

СЕКТОР ЗА ЦЕНТРАЛНА ХАРМОНИЗАЦИЈА НА СИСТЕМОТ НА ВНАТРЕШНА ФИНАНСИСКА КОНТРОЛА ВО ЈАВНИОТ СЕКТОР

НАСОКИ ЗА СПРОВЕДУВАЊЕ НА ИТ РЕВИЗИЈА

СКОПЈЕ, 2025

Содржина:

Вовед

ИТ ревизија : дефиниција, цел и опфат

Предмети за ИТ-ревизија

ИТ-ризиците како основа за ИТ-ревизија

Проценка на контролите поврзани со ИТ

Употреба на критериуми за ревизија и рамки за ИТ-ревизија

АНЕКС 1: Листа за проверка за општи ИТ контроли

Вовед

Со текот на годините, влијанието на информатичката технологија (ИТ) значително се зголеми во средини во јавниот сектор. Во денешно време, речиси и да не постојат процеси или јавни услуги што не се поддржани или примарно управувани од ИТ. Внатрешната ревизија има улога во проценката на степенот до кој овие (автоматизирани) системи се соодветни и доверливи. Со ова упатство се даваат генералните методолошки насоки како се спроведува овој тип на ревизии односно ИТ ревизиите.

Вниманието на ризиците поврзани со ИТ-средината има висок приоритет во Глобалните стандарди за внатрешна ревизија воспоставени од Институтот за внатрешни ревизори (ИИА). Тие ги содржат следните задолжителни аспекти:

Извадок од **Глобалните стандарди за внатрешна ревизија**

Стандард 4.2. Должно професионално внимание
Барања
Внатрешните ревизори мора да покажат должно професионално внимание при проценка на природата, околностите и барањата на услугите што треба да се обезбедат, вклучувајќи и употребата на соодветни техники, алатки и технологија.

Стандард 9.4. План на внатрешна ревизија
Барања
Планот на внатрешна ревизија мора, покрај другото, да ја земе предвид покриеноста на управувањето со информатичка технологија, ризикот од измама, ефективноста на програмите за усогласеност и етика на јавниот субјект, како и други области со висок ризик.

Стандард 10.3. Технолошки ресурси
Барања
Раководителот на единицата за внатрешна ревизија мора да се стреми да обезбеди функцијата за внатрешна ревизија да располага со технологија која го поддржува процесот на внатрешна ревизија и редовно да ја оценува технологијата што ја користи функцијата за внатрешна ревизија и да бара можности за подобрување на ефективноста и ефикасноста.

Стандард 13.5. Ресурси за ангажман
Барања
При планирање на ангажманот, внатрешните ревизори мора да ги идентификуваат видовите и квантитетот на ресурсите потребни за постигнување на целите на ангажманот. Внатрешните ревизори мора да имаат предвид покрај другото дали расположливите финансиски, човечки и технолошки ресурси се соодветни и доволни за постигнување на целите на ангажманот.

Стандард 3.1. Компетентност
Размислувања за спроведување
Внатрешните ревизори покрај другото треба да развијат компетенции поврзани и со деловните функции, како што се финансиски менаџмент и информатичка технологија.

Стандард 9.4. План на внатрешна ревизија
Размислувања за спроведување
За да ја заврши проценката на ризикот низ целата институција, раководителот на единицата за внатрешна ревизија треба да ги земе предвид целите и стратегиите не само на широкото организациско ниво, туку, исто така, и на ниво на посебните единици предмет на ревизија. Дополнително, раководителот на единицата за внатрешна ревизија треба да обрне соодветно должно внимание на ризиците – како што се оние поврзани со етика, измама, **информатичка**

технологија, односи со трети страни, како и неусогласеност со регулаторните барања – коишто може да бидат поврзани со повеќе од една деловна единица или процес и може да бараат посложена проценка.

Стандард 11.1. Градење односи и комуникација со засегнатите страни
Размислувања за спроведување
Раководителот на единицата за внатрешна ревизија може да делегира поединечни внатрешни ревизори да бидат одговорни за одржување постојана комуникација со раководството на клучните функции како што се раководители на деловни сегменти, глобални операции, **информатичка технологија**, финансии, усогласеност и човечки ресурси.

Стандард 14.2 . Анализи и потенцијални наоди од ангажманот
Размислување за спроведување
Внатрешните ревизори треба да разбираат и да користат технологии кои ја подобруваат ефикасноста и ефективноста на анализите, како што се софтверски апликации кои овозможуваат тестирање на целата популација наместо само на примерок.

Глобалните водичи за технолошка ревизија (GTAG®) им обезбедуваат на ревизорите знаење за извршување услуги на уверување или советодавни услуги поврзани со ризиците и контролите на информатичката технологија и безбедноста на информациите на организацијата.

Вниманието дадено на ИТ-ризиците во Глобалните стандарди за внатрешна ревизија јасно покажува дека внатрешната ревизија мора да ги вклучи ризиците поврзани со ИТ во својот делокруг на работа. Ова значи дека анализата/проценката на ризик што ја врши внатрешната ревизија со цел да се изготви годишниот план за внатрешна ревизија мора да ги вклучува овие видови ризици. ИТ-ревизиите може да се планираат и спроведат како ангажмани за поединечна ревизија или како дел од други видови ревизии. На пример, не е невообичаено да се вклучат аспекти поврзани со ИТ во ревизиите на успешност или да се користи вклучување на ИТ во рамките на финансиската ревизија.

Треба да се напомене дека ИТ-ревизијата доаѓа во многу облици и форми. Начинот на кој се спроведува ИТ-ревизијата во одредена средина многу зависи од нивото на зрелост на самата функција на внатрешна ревизија и од степенот до кој се користи информатичката технологија. Затоа, наведените пристапи за ИТ-ревизија во ова упатство се напишани со поглед на нивото на зрелост на внатрешната ревизија во нашата држава, како и на „густината на ИТ“и сложеноста/комплексноста на ИТ- јавен сектор.

ИТ ревизија : дефиниција, цел и опфат

ИТ-ревизијата може да се дефинира и опфати на различни начини. Како што беше споменато претходно, ова во голема мера зависи од средината во која се спроведуваат овие ревизии. Повеќето дефиниции за ИТ-ревизија ги имаат следниве заеднички елементи:

- ИТ ревизијата е испитување и евалуација на инфраструктурата на информатичката технологија, апликациите, користењето и управувањето со податоци, политиките, процедурите и оперативните процеси на субјектот во однос на признаените стандарди или воспоставените политики.
- ИТ-ревизиите оценуваат дали контролите за заштита на средствата на информатичката технологија обезбедуваат интегритет и се усогласени со целите и задачите на субјектот.
- ИТ-ревизиите се користат за да се процени способноста на осубјектот/институцијата да ги заштити своите информациски средства и правилно да ги доставува информациите до овластените страни.

Горенаведените аспекти јасно покажуваат дека ИТ-ревизиите во суштина не отстапуваат многу од било кој друг вид на ревизија: фокусот е на проценката на контролите кои (треба) да обезбедат сигурно и безбедно функционирање на системите кои обезбедуваат и обработуваат информации во рамките на јавниот субјект. Како и во секој друг вид на ревизија, ревизорот ја врши оваа активност од независна и објективна позиција и гледна точка. Резултатот од работата што ја врши ИТ-ревизорот обезбедува уверување на раководството во однос на аспектите што беа оценети.

Предмети за ИТ-ревизија

ИТ-ревизијата може да се фокусира на широк спектар на ревизорски предмети. Некои примери се:

- Техничка инфраструктура (целокупноста на ИТ-системите и нивната организација)
- Оперативен информациски систем
- ИТ-процеси
- Софтвери
- Системи за безбедност
- Заштита на личните податоци.
- Сертификација или акредитација.
- ИТ-проекти / улога во клучни постигнувања/промени
- ИТ-управување, политики и планови

Во исто време, ИТ-ревизиите (дури и кога ИТ-аспектите се дел од друг вид на ревизија) обично се фокусираат на одредени елементи. Вообичаена категоризација е следната:

- **Доверливост** : овластување, идентификација, итн.
- **Интегритет:** комплетност, точност, автентичност на генерираните податоци/информации
- **Достапност** : континуитет, преносливост, обновливост

Доверливост, интегритет и достапност (често наречени ДИД (CIA)) се камен-темелник во ИТ-ревизијата, главно поврзани со (информациски) безбедносни елементи кои во повеќето случаи се составен дел на секоја ИТ-ревизија.

Следното е преглед на трите клучни концепти што ја формираат ДИД:

- **Доверливоста** е приближно еднаква на приватноста. Мерките за доверливост се дизајнирани да спречат обиди за неовластен пристап до чувствителни информации. Вообичаено е податоците да се категоризираат според висината и видот на штетата што би можела да се направи доколку падне во погрешни раце. Потоа, може да се спроведат повеќе или помалку строги мерки според тие категории.
- **Интегритетот** вклучува одржување на конзистентноста, точноста и доверливоста на податоците во текот на целиот животен циклус. Податоците не смеат да се менуваат за време на преносот и мора да се преземат чекори за да се осигура дека податоците не можат да се менуваат од неовластени лица (на пример, со прекршување на доверливоста).
- **Достапноста** значи дека информациите треба да бидат доследно и лесно достапни за овластените страни. Ова вклучува правилно одржување на хардверската и техничката инфраструктура и системи што ги чуваат и прикажуваат информациите.

ИТ-ризиците како основа за ИТ-ревизија

ИТ ризиците се ризици поврзани со употребата, сопственоста, работењето, вклученоста, влијанието и усвојувањето на ИТ во јавниот субјект. ИТ ризиците се состојат од настани поврзани со ИТ кои потенцијално би можеле да влијаат на јавниот субјект и/или на постигнувањето на целите на јавниот субјект. Како што беше споменато претходно, според Глобалните стандарди за внатрешна ревизија, внатрешната ревизија мора да го вклучи потенцијалот за ризици поврзани со ИТ во својот опфат (а со тоа и во планирањето на ревизијата заснована на ризик).

Силно се препорачува да се наведат ризиците поврзани со ИТ не само како посебна активност, туку да се бидат вклучени во проценка на ризиците за потребата на изготвување на годишниот план за внатрешна ревизија.

Ризиците поврзани со ИТ може да се појават/материјализираат во различни области, како на пример:

- Ризици поврзани со безбедноста на информациите / сајбер-безбедноста / приватноста на информациите.
- Ризици поврзани со веродостојноста на информациите генерирани од ИТ-системи (на пример информации генерирани од системите во рамките на финансиската администрација/финансиското работење).
- Ризици поврзани со слабости во контролите вградени во ИТ-системи кои треба да спречат грешки (човечка грешка) или непожелни намерни дејства (како измама/корупција).
- Ризици поврзани со пропусти во организацијата на ИТ низ целиот јавен субјект (се мисли на управување со овластувања, управување со промени, воведување нови ИТ-системи, недостаток на процедури за резервна копија/back up/ и процедури за обновување итн.

Појавата на горенаведените примери за ризик се природно многу зависни од начинот на кој ИТ е организиран и вграден во процедурите на јавниот субјект. Аспектите како сложеноста на системите што се користат, квалитетот на контролите во и околу овие системи, чувствителноста на информациите што течат/поминуваат низ системите, сите ја одредуваат можноста и влијанието на споменатите ризици. Исто така, начинот на кој јавниот субјект се справува со воведувањето на нови ИТ-системи и функционирањето/организацијата на ИТ-секторот влијае на потенцијалната појава на ризици поврзани со ИТ.

Раководството на јавниот субјект треба периодично да биде свесен за потенцијалната појава на ИТ-ризици, исто како и секој друг вид на ризици. Внатрешната ревизија, преку својата сигнална/детективна, уверувачка и консултантска улога, да игра витална улога во обезбедување на

информации за менаџментот. Затоа, ИТ-ризиците може (и треба) да бидат поврзани со соседни области на ризик како што се ризиците поврзани со перформансите/оперативните ризици и финансиските ризици.

Проценка на контролите поврзани со ИТ

При проценка на контролите за време на ИТ-ревизија (или како дел од друг вид ревизија), се прави разлика помеѓу два вида на контроли:

А. ИТ-општи контроли
Б. Контроли на апликацијата

А) ИТ-Општи контроли:

ИТ-генералните контроли се оние контроли кои обезбедуваат добро функционирање на таканаречената ИТ-инфраструктура[1], севкупноста на сите ИТ-системи во јавниот субјект. ИТ-општите контроли може да се гледаат/сметат како организациски процеси кои го регулираат и контролираат начинот на кој се користи ИТ. Очигледна претстава за ИТ-општите контроли обично е опфатена во улогите и одговорностите на ИТ-одделот. Типични контроли што се дел од областа на ИТ-општите контроли се:

- **Управување и раководење со ИТ:** се однесуваат на стратешката и раководната страна на ИТ. Тоа се однесува на пример постоењето на стратешки ИТ-план, општото управување со ИТ, позиционирањето и функционирањето на ИТ-одделот/единицата и постоењето на управување со ИТ-ризици.
- **Управување со податоци:** политики и процедури што обезбедуваат дека податоците/информациите на јавниот субјект се чуваат и одржуваат на сигурен и безбеден начин, гарантирајќи дека аспектите како што се доверливост, интегритетот и пристапноста се добро избалансирани.
- **Управување со овластувања** : регулирање кој има пристап до кои информации (и поврзаните системи со нив)
- **Управување со инциденти** : се однесува на процедурите што треба да се воспостават во случај на ад-хок инциденти во рамките на ИТ-инфраструктурата. Пример е вработен со заклучена сметка на која треба да се обрати или софтверска програма што се замрзнува.
- **Управување со лозинки** : осигурување дека секој вработен има единствена лозинка и дека е обезбедено ажурирање/обновување на лозинките.
- **Управување со пристап:** не се однесува само на обезбедување/регулирање на овластен пристап до ИТ-системи, туку и на тоа кој има физички пристап, на пример, до сервер собата или кој има пристап до просториите на јавниот субјект (на пр. контролиран со клуч-картички).
- **Управувањето со промени** се однесува на процедурите и политиките кои обезбедуваат непречена транзиција/премин кога се иницираат промени во ИТ инфраструктурата. Размислете на пример за воведување на нов ИТ-систем или премин на нова веб-страница за јавниот субјект.
- **Процедури за резервна копија и обновување:** оние процедури и контроли кои обезбедуваат континуитет во работењето во случај клучните ИТ системи да пропаднат или да престанат да работат.
- **Поделба на должностите:** се однесува на политиките, процедурите и управувачката структура за управување и контрола со доделување на одделни поединци одговорноста за иницирање и евидентирање трансакции (на пример во рамките нафинансиското работење).

[1] ИТ-инфраструктурата се однесува на севкупноста на процесите управувани од ИТ, нејзините системи и операции во рамките на јавниот субјект

- **Процедури и политики за безбедност на информациите:** Терминот „безбедност на информации“ се однесува на сите практики, процеси и алатки кои се користат за заштита на информациските средства и системи најавниот субјект. Од клучно значење е да се имплементираат стандардизирани форми на безбедност на информациите, за да се осигура дека информациите остануваат безбедни и заштитени. Ова обично вклучува процеси кои спречуваат губење на податоци од секаков вид, вклучувајќи кражба на податоци, ексфилтрација и корупција, и случајна модификација, како и процеси кои штитат од познати сајбер закани и техники и стратегии за справување со непознати сајбер-напади.
- **Аутсорсинг (аспекти на) ИТ инфраструктура:** се занимава со политиките, процедурите и контролите поврзани со надворешните аспекти на ИТ префрлени на трети страни. Пример може да биде складирањето на податоци во облак (cloud) - услуги.

Аспектите споменати погоре (треба) да се потпираат на процедури и политики. Вообичаено, овие процедури и политики се засноваат на рамки за најдобра практика кои обезбедуваат насоки за дизајнирање и спроведување на општи контроли за ИТ. За внатрешниот ревизор, овие рамки може да се користат како критериуми за проценка на општите контроли. Анекс 1. дава преглед на специфични проверки кои внатрешниот ревизор може да ги изврши при проценка на ИТ-општите контроли. Овие проверки се засноваат на критериуми кои произлегуваат од рамката COBIT [2], рамка за управување со ИТ за организации/субјекти кои сакаат да ги имплементираат, следат и подобрат најдобрите практики за управување со ИТ. COBIT-рамката ги категоризира ИТ-општите контроли во:

1. Управување и раководење со ИТ
2. Управување со податоци
3. Планирање на континуитет на работењето (вклучува политики за резервна копија и обновување)
4. Безбедност на информации
5. Управување со промени
6. Аутсорсинг на ИТ инфраструктура

При проценка на општите ИТ-контроли, ИТ-ревизорот во принцип не треба да поседува длабоко познавање на техничките работи поврзани со ИТ-системи. Се разбира, помага доколку ревизорот има општо разбирање за тоа како е организирана ИТ-инфраструктурата и кои политики, процедури и засегнати страни играат улога во нејзиното функционирање. Листата за проверка во Анекс 1. покажува дека многу аспекти кои (може да се проценат) е многу добро возможно да се интегрираат во веќе постоечките рамки за ревизија што ги користат ревизорите (на пример во ревизии на успешност или финансиски ревизии). Силно се препорачува секоја ревизија да определи кои елементи од списокот за проверка на општата ИТ-контрола на рамката COBIT се соодветни да се вклучат во планираните ревизии.

Исто така, треба да се забележи дека политиките и процедурите треба да ги исполнуваат луѓето/вработените, поддржани од ИТ. Овие аспекти може да се опфатат преку, на пример, интервјуа и преглед со фокус на контролите на апликациите (види следно поглавје). Во нашиот контекст, засега се препорачува прво да се утврди како и до кој степен аспектите на општите ИТ-контроли може да се вклучат во работата на внатрешната ревизија.

ИТ-ревизијата го разгледува дизајнот на општите ИТ-контроли и оперативната ефективност:

При проценка на општите ИТ-контроли, ИТ-ревизорот не треба само да го погледне дизајнот на контролите (на пример, само со прегледување на политиките и процедурите на хартија), туку треба да

[2] COBIT кратенка за: Контролни цели за информатичка технологија. Оваа рамка е развиена од ISACA, глобалната асоцијација која на ИТ професионалците им обезбедува знаење, ингеренции, обука и заедница за ревизија, управување, ризик, приватност и сајбер-безбедност. www.isaca.org

ја разгледа и таканаречената оперативна ефикасност (како тоа работи во пракса). За ова, како и во секој друг вид ревизија, се советува да се вклучат информации преку интервјуирање или други техники како што се набљудување.

Б) Контроли на апликацијата

Контролите вградени во апликациите за работни процеси најчесто се нарекуваат *контроли на апликации/апликациски контроли*. Апликациските контроли се однесуваат на контролите на обработката на трансакциите и податоците во рамките на апликативниот систем (на пример во софтверска програма што се користи при набавките) и затоа се специфични за секоја апликација. Додека општите ИТ контроли во еден субјект го поставуваат тонот за целокупното контролна средина за информациските системи, контролите на апликациите се вградени во специфични апликации за да се обезбеди и заштити комплетноста, точноста, валидноста, интегритетот, веродостојноста и доверливоста на информациите. Затоа, целите на контролите на апликацијата генерално вклучуваат обезбедување на:

➢ Подготвените податоци за внесување/внесувањето на комплетни/целосни, валидни и веродостојни
➢ Податоците се конвертираат во автоматизирана форма и се внесуваат во апликацијата точно, целосно и навреме
➢ Податоците се обработуваат од апликацијата целосно и навреме, и во согласност со утврдените барања
➢ Излезот е заштитен од неовластена модификација или оштетување и се дистрибуира во согласност со пропишаните политики

Контролите на апликацијата имаат важна улога во средината за обработка на информации за да се обезбеди доверливост, интегритет и достапност на информациите. Во општата контролна средина која е релативно добро поставена, ревизорот треба да добие уверување дека трансакциите се правилно иницирани, одобрени, обработени и евидентирани. Бидејќи контролите на апликациите/апликативните контроли се тесно поврзани со поединечни трансакции, полесно е да се види зошто тестирањето на контролите ќе му обезбеди на ревизорот уверување за точноста на одредено салдо на сметката.

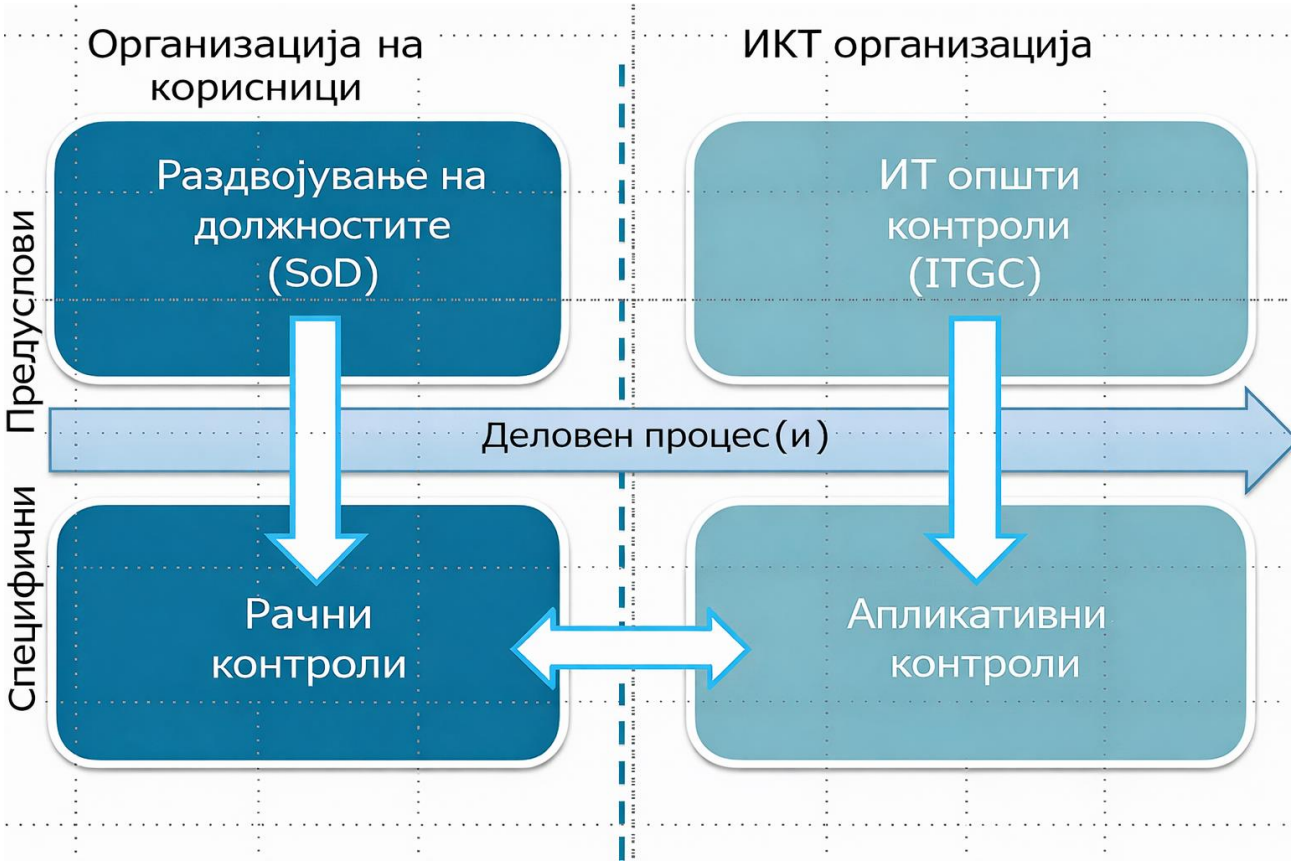
Некои клучни видови на контроли на апликациите се:

- Контроли за внесување – Овие контроли се користат главно за проверка на интегритетот на податоците внесени во апликацијата за работа, без разлика дали податоците се внесени директно од вработените, од далечина од деловен партнер или преку веб-овозможена апликација или интерфејс. Внесувањето на податоците се проверува за да се осигура дека тие остануваат во рамките на одредените параметри.
- Контроли на обработка - Овие контроли обезбедуваат автоматизирани средства за да се осигура дека обработката е целосна, точна и овластена.
- Излезни контроли/Контроли на излез- аутпут - Овие контроли се однесуваат на она што е направено со податоците и треба да ги споредат излезните резултати со планираниот резултат со проверка на излезот во однос на влезот.
- Контроли за интегритет - овие контроли ги следат податоците што се обработуваат и се складираат за да се осигураат дека тие остануваат конзистентни и точни.
- Патека за управување/Управувачка трага – Контролите на историјата на обработка, честопати наречени ревизорска трага, му овозможуваат на раководството да ги идентификува трансакциите и настаните што ги снима преку следење на трансакциите од нивниот извор до нивниот излез и со следење наназад. Овие контроли, исто така, ја следат ефективноста на другите контроли и ги идентификуваат грешките што е можно поблиску до нивните извори.

Оценувањето/тестирањето на контролите на апликациите бара подлабоко разбирање на ИТ, неговите системи и софтверот што се користи. Употребата на ИТ-алатки за ревизија е вообичаена практика при оценување на контролите на апликациите.

Споредба на општи контроли и контролите на апликации

ИТ општите контроли и контролите на апликациите треба да бидат добро избалансирани. Доколку општата функција на ИТ функционира на соодветен начин, голема е можноста контролите на апликацијата да бидат вградени во работните процеси и функцијата на софтверот исто така на добар начин. Во ревизорското опкружување/средина со најдобра практика, и двете треба да бидат оценети од внатрешниот ревизор за да се добие целосна слика. Во шемата/графиконот подолу е наведена , поврзаноста помеѓу ИТ општите контроли и контролите на апликацијата . Предусловите за добро функционална ИТ инфраструктура се одредуваат според тоа како функционираат општите ИТ контроли. Ова може да се оцени (на пример) со користење на критериумите во Анекс 1. Општите контроли на ИТ треба да ја одразуваат поделбата на должностите во клучните/чувствителните/ризичните процеси во таканаречената организација на корисници (на пример во процесот на набавка). Истовремено, внатрешните контроли кои ја поддржуваат поделбата на должностите исто така треба да бидат вградени во внатрешните процеси (корисничка организација) како и во контролите на апликацијата во софтверот што се користи. Така, графиконот го покажува меѓусебната поврзаност помеѓу организацијата (корисникот), контролната средина и како тоа се пресликува во општите контроли на ИТ и контролите на апликациите.



За контекстот на нашата држава, се советува најпрво да се започне со фокусирање на стекнување искуство во проценката на општите контроли на ИТ (со користење на COBIT-критериумите во Анекс 1.). Проценката на контролите на апликацијата бара дополнителни вештини кои можат да се стекнат со текот на времето кога функцијата на внатрешна ревизија ќе се развива понатаму и кога/ако може да се создадат специјализации во рамките на ИТ-ревизија.

Употреба на критериуми за ревизија и рамки за ИТ-ревизија

Критериумите за ревизија во ИТ-ревизијата често се изведуваат од т.н. рамки за ИТ-ревизија. Во претходниот став, COBIT беше споменат како пример за таква рамка. За специфични цели во ИТ-ревизијата, достапни се различни можни рамки со групи на критериуми за ревизија. Понекогаш, овие групи на критериуми може да се комбинираат или да се прилагодат на специфична ситуација или специфично барање.

За да ја избере вистинската рамка, ИТ-ревизорот треба да одлучи која рамка е најсоодветна во однос на ИТ-предметот. На пример:

- CobIT (обезбедува стандарди засновани на најдобрата практика за управување со ИТ)
- ITIL (управување со ИТ услуги)
- Prince2 (управување со проекти: корисно при оценување на ИТ-проект)
- ISO27001/2 (Информациска безбедност)
- Услуги на софтвер за најдобри практики (CIS; NIST)
-

Во овие рамки, ИТ-ревизорот може да ги избере вистинските информации за да ги утврди критериумите за ревизија со следење на следните чекори:

1. „Разберете го работењето“: Собирање на релевантни информации за разбирање на јавниот субјект и нејзината ИТ-инфраструктура, апликации, ИТ-процеси, ИТ-организација итн.
2. Идентификувајте и класифицирајте ги ризиците поврзани со ИТ-целите и опфатот на ИТ-ревизијата. На пример: ако опфатот е „безбедност“, ризиците за губење на доверливоста, интегритетот и достапноста на информациите се релевантни. Но, кога на пример „достапноста“ не е во опфатот на ИТ-ревизијата, не е неопходно да се преземе следниот чекор во врска со достапноста.
3. Изберете ги контролните мерки што би очекувале да бидат во ИТ организацијата и ИТ системот во однос на ИТ предметот. Ова се критериумите за ревизија што ќе ги користи ИТ ревизорот.
4. Изградете ја рамката за ИТ ревизија со овие критериуми за ревизија

АНЕКС 1: Листа за проверка за општи ИТ контроли

Потребно е да се процени ИТ контролната средина како основа за одлучување колку ревизијата ќе се потпира на податоците произведени/изготвени од компјутеризирани ИТ системи. Слабостите во ИТ контролната средина имаат големо влијание врз сите апликации и податоци што се одржуваат во таа средина.

Оваа листа за проверка за општи контроли е збир на прашања од затворен тип за употреба во ограничен преглед на ИТ контролната средина кај субјектот кој е предмет на ревизија. Таа ќе им помогне на ревизорите да ги проверат главните цели за ИТ контрола, кои се засноваат на рамката COBIT во однос на регулаторната рамка на ЕУ и критериумите за информации во областите на управување и раководење со ИТ, управување со податоци, планирање на континуитет на работењето, безбедност на информации, управување со промени и аутсорсинг на ИТ инфраструктура. *Повикувањата/референците кон рамката за COBIT и регулаторната рамка на ЕУ, се дадени индикативно, со цел да ги претстават меѓународните/европските практики во оваа област, истите при практично користење на листата за проверка од страна на ревизорскиот тим може да бидат отстранети. Листата за проверка може при употреба може да се прилагоди на специфичностите на јавниот субјект, притоа да се внимава содржината на истата да не отстапува од Рамката за внатрешна ревизија*

согласно којашто треба да се врши внатрешната ревизија, а истото е утврдено со Законот за системот на внатрешна финансиска контрола во јавниот сектор.

Можете да преминете директно (со користење на линкот) на следните делови од списокот за проверка за општите контроли:

1. Управување и раководење со ИТ
2. Управување со податоци
3. Планирање на континуитет на бизнисот
4. Безбедност на информации
5. Управување со промени
6. Аутсорсинг на ИТ инфраструктура

1) УПРАВУВАЊЕ И КОНТРОЛИ НА УПРАВУВАЊЕТО

	Контролни цели и повикување на регулаторната рамка	**COBIT ref.**	**Тестови на контроли**	**Евалуација**	**Потребни документи**
1.	***Контролна цел:*** *ИТ стратегијата е усогласена и ја поддржува целокупната стратегија на јавниот субјект* ***Референци за регулаторна рамка:*** *FR Чл 28a(2)(a) и 27(3); ICS7* ***Критериуми за поврзани информации:*** *Ефективност и ефикасност*	PO1.4 PO1.5	1. Дали постои повеќегодишна **ИТ стратегија или ИТ план** (3-5 години) што е формално одобрен на соодветно ниво? 2. Дали ИТ стратегијата има соодветни и релевантни цели, буџет и индикатори за успешност? 3. Дали постојат ИТ годишни работни програми во согласност со ИТ стратегијата?		• ИТ стратегија или ИТ план • ИТ годишни работни програми

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни документи
2.	***Контролна цел :*** *Направете ефективни и ефикасни ИТ инвестиции и поставете и следете буџети за ИТ во согласност со ИТ стратегијата и инвестициските одлуки.* ***Референци за регулаторна рамка:*** *FR чл. 27 (3); ICS7* ***Критериуми за поврзани информации:*** *Ефективност и ефикасност*	PO5.3 PO5.4 DS6.3	1. Дали трошоците за ИТ се планираат, управуваат и следат во рамките на годишен буџет кој е усогласен со ИТ стратегијата и доволно детален за да ги одрази приоритетите на јавниот субјект?		• Годишен буџет за ИТ (посебен или дел од општиот буџет на јавниот субјект) • Сите документи за следење на годишниот буџет за ИТ

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни документи
3.	***Контролна цел:*** *Обезбедете точни, разбирливи и одобрени политики, процедури и упатства, вградени во рамка за ИТ контрола.* ***Референци за регулаторна рамка:*** *ICS8 и ICS12* ***Критериуми за поврзани информации:*** *Ефективност*	PO6.3 PO6.4 PO6.5	1. Дали постојат напишани и формално одобрени политики и/или процедури кои ги покриваат повеќето клучни аспекти од управувањето со ИТ: a. Управување со податоци и класификација? b. континуитет на работењето? c. Безбедност на информации? d. Ризици и контроли? e. Управување со промени?		• Политики, процедури, упатства и прирачници

4.	***Контролна цел:*** *Воспоставување транспарентни, флексибилни и одговорни ИТ организациски структури и дефинирање и спроведување на ИТ процеси обезбедени со носители, улоги и одговорности.* ***Референци за регулаторна рамка:*** *FR чл. 28a(2)(a); ICS3, ICS7 и ICS8.* ***Критериуми за поврзани информации:*** *Ефективност и ефикасност*	PO4.1 PO4.3 PO4.4 PO4.5 PO4.6 PO4.8 PO4.11 PO7.1 PO7.4 PO7.8 ME3.1	1. Дали одделот за ИТ е соодветно поставен во организацијата, со оглед на големината и мисијата на организацијата? 2. Дали постои управен одбор за ИТ составен од извршни, деловни и ИТ менаџмент/раководството и задолжени за обезбедување усогласување на работењето (со надзор на ИТ плановите и политиките) и следење на ИТ услугите и проектите? 3. Дали ИТ процесите и улогите и одговорностите специфични за ИТ се правилно дефинирани, реализирани и следени? 4. Дали е назначен службеник за безбедност на информации (LISO) и офицер за локална безбедност (LSO) во согласност со регулаторната рамка на Комисијата? 5. Дали постојат политики и процедури за управување со регрутирање на персонал и престанок на работа?		• Рамка за ИТ процес, документирани улоги и одговорности • Описи на ИТ работни места • Политика и процедури за ИТ човечки ресурси • Одлука или друг документ во врска со формирањето на управен комитет за ИТ • Примерок записник од состаноците на ИТ управниот комитет

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни документи
			6. Дали следните улоги се одделени/одвоени: a. Безбедност: службеник за безбедност (LSO и LISO) – сопственик на системот – администратор за безбедност (LSA-Локален безбедносен администратор)? b. Промени: развој – тестирање – обезбедување квалитет – производство?		

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни документи
5.	***Контролна цел:*** *Идентификување, приоретизирање, ограничувањ/намалувањее или прифаќањее/главните ризици кои произлегуваат одо областа на ИТ и поврзанитее функции.* ***Референци за регулаторна рамка:*** *IR чл. 48 (д); ICS6 и ICS12* ***Критериуми за поврзани информации:*** *доверливост, интегритет и достапност*	PO9.1 PO9.2 PO9.3 PO9.4 PO9.5	1. Дали ИТ ризиците се управуваат во согласност со рамката за управување со ризик на јавниот субјект? 2. Дали постои **рамка за управување со ризик специфична за ИТ** ? 3. Дали ИТ ризиците се дефинираат и редовно се следат во **евиденцијата/регистарот за ИТ ризик** (одделно или во рамките на регистарот на ризиците на јавниот субјект)?		• Рамка и/или политика за управување со ризик • Евиденција-регистар/мапа на ИТ ризик

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни документи
6.	***Контролна цел:*** *Идентификување, спроведување и следење на процес на внатрешна контрола за активностите поврзани со ИТ.* ***Референци за регулаторна рамка:*** *FR чл. 28a(2)(a,b,c); IR уметности 22a и 48(д); ICS9, ICS11, ICS 12 и ICS15* ***Критериуми за поврзани информации:*** *Ефективност и ефикасност*	ME2.1 ME2.2 ME2.7 ME3.1	1. Дали е воспоставен сет на ИТ контроли усогласени со рамката за внатрешна контрола на јавниот субјект? 2. Дали е идентификуван сет на ИТ контроли дизајнирани да ги намалување ИТ ризиците? 3. Дали има редовно следење и известување за ефективноста на ИТ контролите? 4. Дали организацијата на ИТ е во согласност со важечките правила и прописи во области како што се заштитата на податоците и правата на интелектуална сопственост? 5. Дали се изготвени внатрешни или надворешни ревизорски извештаи за областа на ИТ/ теми?		• Документација на внатрешни ИТ контроли или стандарди за внатрешна контрола на јавниот субјект (на пр. ИКС во Европската Комисија) • Ревизорски извештаи од областа на ИТ (последните 3 години)

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни документи
7.	***Контролна цел :*** *Дефинирајте пристап за управување со програма и проект кој е применлив за сите ИТ проекти, овозможува учество на засегнатите страни и ги следи ризиците и напредокот на проектот.* ***Референци за регулаторна рамка:*** *ICS7* ***Критериуми за поврзани информации:*** *Ефективност и ефикасност*	PO10.2 PO10.3 AI2.2 AI4.3 AI4.4	1. Дали постои методологија за управување со ИТ проекти? 2. Дали ИТ проектите се управуваат во согласност со методологијата за управување со проекти? 3. Дали новите ИТ системи се развиени во согласност со методологијата за развој на софтвер (на пр. RUP@EC)?		• Упатство/документација за управување со проекти • Методологија за развој на софтвер
8.	***Контролна цел :*** *Следење и известувајње за метриките на процесот и идентификување и имплементирање активности за подобрување на перформансите.* ***Референци за регулаторна рамка:*** *IR чл. 22а(1)(д); ICS9 и ICS15* ***Критериуми за поврзани информации:*** *Ефективност и ефикасност*	ME.1.1 ME.1.4 ME.1.5 ME.4.1 ME.4.2	1. Дали на повисокото раководство (или на управниот одбор) им се даваат редовни **извештаи** за напредокот за севкупниот придонес на ИТ во работењето, за да можат да го следат степенот до кој се постигнати планираните цели, користените буџетски ресурси, се исполнети целите за перформанси и идентификуваните ризици се намалени?		• Редовни извештаи за напредокот

2) КОНТРОЛИ ЗА УПРАВУВАЊЕ СО ПОДАТОЦИ

	Контролни цели и повикување на регулаторната рамка	**COBIT ref.**	**Тестови на контроли**	**Евалуација**	**Потребни документи**
1.	***Контролна цел:*** *Осигурување дека податоците се правилно зачувани, архивирани и отстранети.* ***Референци за регулаторна рамка:*** *FR чл. 28a(2)(b,c); IR чл 22a(1)(d), 48(f,g), 107 и 108; ICS10, ICS11, ICS12 и ICS13* ***Критериуми за поврзани информации:*** *Интегритет*	DS11.2 DS11.4 DS11.5 DS11.6	1. Дали постојат правила за зачувување на документи, податоци и изворни програми во согласност со активностите, големината и мисијата на јавниот субјект? 2. Дали постојат соодветни политики и процедури за резервна копија на системите, апликациите, податоците и документацијата: a. Дали процедурите за резервна копија обезбедуваат гаранции за обновување на податоците (со фреквенции, копии, проверки итн.) и одговараат на планот за континуитет на работењето? b. Дали се прават резервни копии на сите релевантни податоци (на пр. со помош на ревизорски дневници, документи, табели)? c. Дали има добро дефинирана логичка и физичка безбедност за изворите на податоци и резервните копии? d. Дали е доделена одговорност за правење и следење на резервните копии? 3. Дали системите, апликациите, податоците и документацијата одржувани или обработувани од трети страни имаат соодветни резервни копии и/или се обезбедни? ? 4. Дали организацијата има политики за да обезбеди заштита на чувствителните податоци и софтвер кога податоците и хардверот се отстрануваат или пренесуваат? 5. Дали периодите на задржување на податоците се во согласност со договорните, законските и регулаторните барања?		• Политика за управување со податоци • Резервни процедури • Процедури за отстранување на медиумите • Договори со трети страни или договори на ниво на услуги (клаузули за управување со податоци)

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни документи
2.	***Контролна цел:*** *Воспоставување модел на податоци за јавниот субјект кој вклучува модел за класификација на податоците за да се обезбеди интегритет и конзистентност на сите податоци.* ***Референци за регулаторна рамка:*** *FR чл. 28a(2)(b,c); IR чл 22a(1)(d), 48(c,f) и 107; ICS11, ICS12 и ICS13* ***Критериуми за поврзани информации:*** *Доверливост и интегритет*	PO2.3 PO2.4 DS5.11 DS11.1	1. Дали е дефиниран речник на податоци за да може да се идентификува вишокот/некомпатибилноста на податоците и да се споделат податочните елементи меѓу апликациите и системите? 2. Дали речникот на податоци се применува на постоечки системи, проекти за развој на апликации и големи промени во ИТ апликациите? 3. Далисе идентификувани сопствениците за секој елемент од податоците (датотеки, папки/фолдери, апликации итн.)? 4. Дали податоците се класифицирани според критериумот за информации: a. **доверливост** (јавна, ограничена, итн.); b. **интегритет** (умерен, чувствителен, итн.); c. **достапност** (умерена, критична, итн.)? 5. Дали постои документ кој ја прикажува класификацијата на секој елемент на податоците во согласност со моделот за класификација на податоците?		• Политика за управување со податоци • -Модел за класификација на податоци • Доделени класификации на податоци • Речник на податоци

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни документи
3.	***Контролна цел (не-COBIT):*** *Обезбедување на изготвување на веродостојни финансиски и раководни информации.* ***Референци за регулаторна рамка:*** *FR чл. 28а2(б) и 61(д);* ***IR чл. 48 (ѓ);*** *ICS12 и ICS13* ***Критериуми за поврзани информации:*** *Доверливост и интегритет*	AC2 AC5	1. Дали се дизајнирани контроли за да се обезбеди веродостојност на компјутеризираните податоци, со **изворни документи** ? 2. Дали контролите се дизајнирани да обезбедат **интегритет** и **безбедност** на документи или датотеки (како табеларни пресметки) кои се чуваат на персонални компјутери или споделени дискови и на се потпира јавниот субјект во нејзиниот финансиски работен тек каде што: a. тие датотеки се користат за собирање финансиски податоци или пресметки и служат како основа за **рачни внесувања во финансиските системи** (на пр. ABAC) **наместо како изворни документи** ? b. досиејата се користат за **финансиско известување** ?		

3) КОНТРОЛИ НА ДЕЛОВЕН КОНТИНУИТЕТ

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни документи
1.	***Контролна цел:*** *Изградет/Креирање на/ ги можностите за извршување на секојдневните автоматизирани работни активности со минимален, прифатлив прекин.* ***Референци за регулаторна рамка:*** *CP чл. 28a(2)(в); IR чл. 48 (в); ICS10* ***Критериуми за поврзани информации:*** *Достапност и ефективност*	DS2.5 DS4.2 DS4.3 DS4.4 DS4.5	**1.** Дали има писмен и формално одобрен **план за (обезбедување) континуитет на работењето (BCP)** и **план за обновување од катастрофи (DRP)** ? 2. Дали BCP – ПКР опфаќа: a. Анализа на влијанието на/врз работењето (БИА)? b. Сите клучниработни функции и процеси? c. Улоги, одговорности и процеси на комуникација? 3. Дали тестовите за BCP (планот за обезбедување на континуитет на работењето) се закажани и завршени на редовна основа? 4. Дали BCP- планот за обезбедување на континуитет на работењето се ажурира така што постојано ги одразува реалните барања на работењето? 5. Дали сите критични медиуми за резервна копија, документација, податоци и други ИТ ресурси потребни за ИТ обновување се складирани на надворешна од локацијата? 6. Дали BCP (планот за обезбедување на континуитет на работењрто- и DRP(план за обновување/опоравување од катастрофа) ги дефинираат целите на точките за враќање/опоравување? (**RPOs - recovery point objectives**) и целите за времето на опоравување (**RTOs-recovery time objectives**)? 7. Дали резервните политики се дефинирани во согласност со RPO – целите на точката за опоравување/обновување и RTO-целите на времето за опоравување?		• BCP и DRP • Тест извештаи

Забелешка: во отсуство на соодветен BCP (план за обезбедување на континуирано работење), субјектот кој е предмет на ревизија треба да биде информиран за ризикот без одлагање.

4) КОНТРОЛИ НА БЕЗБЕДНОСТА НА ИНФОРМАЦИИТЕ

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни се документи
1.	***Контролна цел:*** *Воспоставување и одржување улоги, одговорности, политики, стандарди и процедури за ИТ безбедност.* ***Референци за регулаторна рамка:*** *CP чл. 28a(2)(в); IR чл. 48 (в); ICS12* ***Критериуми за поврзани информации:*** *Доверливост, интегритет и ефективност*	PO6.3 DS5.1 DS5.2	1. Дали е изготвена и одобрена политика и/или план за ИТ безбедност на соодветно ниво? 2. Дали планот за **ИТ безбедност го** вклучува/покрива следното: a. Комплетен сет на безбедносни политики и стандарди во согласност со воспоставената рамка за ИТ безбедносна политика? b. Процедури за спроведување и зајакнување на тие политики и стандарди? c. Улоги и одговорности? d. Барања заекипирање? e. Безбедносна свест и обука? f. Извршни постапки/постапки за спроведување? g. Инвестирање во потребните безбедносни ресурси?		• ИТ безбедносна политика и/или план • Релевантни безбедносни политики и процедури

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни се документи
2.	***Контролна цел:*** *Спроведување процедури за контролирање на пристапот врз основа на потребата на поединецот да прегледува, додава, менува или брише податоци.* ***Референци за регулаторна рамка:*** *CP чл. 28a(2)(в); IR чл. 48 (в); ICS12* ***Критериуми за поврзани информации:*** *Доверливост и интегритет*	DS5.3 DS5.4	1. Дали постојат процедури за дефинирање на правата за пристап (преглед/додавање/промена/бришење) до финансиските системи (ABAC, итн.) и податоци/документи?		• Политика за права на пристап на корисниците/Политика за управување со корисници • Списоци за контрола на пристап (за финансиски системи и податоци)
3.	***Контролна цел:*** *Осигурување дека сите корисници (внатрешни, надворешни и привремени) и нивната активност на ИТ системи се единствено/уникатно препознатливи.* ***Референци за регулаторна рамка:*** *CP чл. 28a(2)(в); IR чл. 48 (в); ICS12* ***Критериуми за поврзани информации:*** *Доверливост и интегритет*	DS5.3 AC6	1. Дали постојат механизми за автентикација и авторизација, како што се лозинки, токени или дигитални потписи, за спроведување на правата за пристап според чувствителноста и критичноста на информациите? 2. Дали идентификациитесе единствени и индивидуални и лозинките се познати само на засегнатите лица?		

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни се документи
4.	***Контролна цел:*** *Контролите за соодветната поделба на должностите за барање и давање пристап до системите и податоците постојат и се следат.* ***Референци за регулаторна рамка:*** *CP чл. 28a(2)(в); IR чл. 48 (в); ICS8* ***Критериуми за поврзани информации:*** *Доверливост и интегритет*	DS5.3 DS5.4 PO4.11	1. Дали правата за пристап на корисниците се бараат од раководството на корисниците, одобрени од сопствениците на системот/податоците и имплементирани од *администраторот за безбедност* ? 2. Дали следните улоги се одделени: a. ***Инфраструктура*** : службеник за безбедност (LSO и LISO) – сопственик на системот – администратор за безбедност (имплементира пристап од LSA итн.)? b. ***Апликации*** : сопственик на системот (овластување и следење) – администратор за безбедност(на пр. администратор на профил во ABAC)?		• Списоци за контрола на пристап (за финансиски системи и податоци) • Опис на работните места

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни се документи
5.	***Контролна цел:*** *Осигурајте се дека едно лице (администраторот за безбедност) е одговорно за управување со сите кориснички сметки и безбедносни токени (лозинки, картички, уреди итн.) и дека се дефинирани соодветни процедури за итни случаи. Периодично прегледувајте/потврдувајте ги неговите/нејзините постапки иовластувања.* ***Референци за регулаторна рамка:*** *CP чл. 28a(2)(в); IR чл. 48 (в); ICS8 и ICS12* ***Критериуми за поврзани информации:*** *Доверливост и интегритет*	DS5.4 DS13.4	1. Дали има *службеник за безбедност* задолжен за ИТ безбедноста на јавниот субејкт кој го добива своето овластување од високото раководство? 2. Дали само *службеникот за безбедност* може да управува со кориснички сметки и лозинки? 3. Дали дејствијата на *администраторот за безбедност* периодично се прегледуваат (од LISO), при што се посветува внимание на поделбата на должностите?		• Опис на работните места на службеник за безбедност и администратор за безбедност

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни се документи
6.	***Контролна цел:*** *Обезбедување и одржување соодветна физичка средина за заштита на ИТ средствата од пристап, оштетување или кражба.* ***Референци за регулаторна рамка:*** *CP чл. 28a(2)(в); IR48(в) и 108; ICS12* ***Критериуми за поврзани информации:*** *Доверливост и интегритет*	DS12.2D S12.3 DS12.5	1. Дали е дефинирана и дали се спроведува политика во врска со мерките за физичка безбедност и контрола на пристапот што треба да се следат за да се спречи пожар, оштетување од вода, прекин на струја, кражба итн. во ИТ простории? 2. Дали пристапот до ИТ простории (ИТ соби и објекти)одобрен, ограничен и одземен во согласност со политиките за физичка безбедност? 3. Дали постои процедура за евидентирање и следење на целиот пристап до просториите за ИТ (вклучувајќи ги и изведувачите идобавувачите)?		• Политики кои се однесуваат на физичка безбедност

5) ПРОМЕНИ НА КОНТРОЛИТЕ НА УПРАВУВАЊЕТО

	Контролни цели и повикување на регулаторната рамка	**COBIT ref.**	**Тестови на контроли**	**Евалуација**	**Потребни документи**
1.	***Контролна цел:*** *Контрола на проценката на влијанието, овластувањето и спроведувањето на сите промени во ИТ инфраструктурата, апликациите и техничките решенија; минимизирајте ги грешките поради нецелосни спецификации на барањето; и да се запре имплементацијата на неовластени промени.* ***Референци за регулаторна рамка:*** *IR уметности 22a(1)(г) и 107; ICS8* ***Критериуми за поврзани информации:*** *Интегритет, достапност, ефективност и ефикасност*	AI6.1 AI6.2 AI6.3 AI6.4 AI6.5 AI6.6	1. Дали постои формално одобрена, имплементирана и надгледувана рамка/процедури за управување со промените на ИТ апликациите, програмите и базите на податоци? 2. Дали рамката за управување со промени вклучува/покрива: a. Улоги и одговорности? b. Промена на процедурите за барање? c. Проценка на ризиците и влијанијата од промените? d. Овластувања од страна на раководството за брања за промени? e. Одобрување од клучните/главните засегнати страни, како што се корисниците и сопствениците на системот, пред промените да преминат во ? f. Преглед н и одобрување од раководството на промените пред тие да преминат воупотреба? g. Класификацијата на промените (големи, помали, итни промени итн.)? h. Следењето на промените? i. Механизми за контрола на верзии? j. Дефиницијата на процедурите за враќање назад? k. Употреба на процедури за итна промена? l. Ревизорски траги?		• Рамка/процедури за управување со промени • Сите записи на примерок од промени (од дневникот на барања за промени до преминување вокористење/употреба)

			3. Дали се почитуваат следниве критериуми за поделба на должностите во контекст на програмските промени: a. Дали е јасно утврдена поделбата на должностите за развој, тестирање, обезбедување квалитет и производствени задачи? b. Дали развивачите на програми и тестери спроведуваат активности само за „тест“ податоци? 4. Дали крајните корисници или системските оператори имаат директен пристап до изворните кодови на програмата?		
2	***Контролна цел:*** *Тестирање дали апликациите и инфраструктурните решенија се соодветни за целта на намената и без грешки и дали е извршена соодветна конверзија на податоците.* ***Референци за регулаторна рамка:*** *IR Arts 22a(1)(d) и 107; ICS8* ***Критериуми за поврзани информации:*** *Ефективност*	АИ7.2 АИ7.6	1. Дали сите големи промени се тестираат во однос на функционалните и оперативните барања за да се осигура дека се постигнати првичните работни цели? 2. Дали сите големи промени се извршени во согласност со план за тестирање кој опфаќа: a. Организациски стандарди, улоги и одговорности? b. Подготовка за тестирање, вклучително и подготовка на локацијата? c. Барања за обука, доколку е потребно? d. Инсталација или ажурирање на дефинирана околина/средина за тестирање? e. Планирање/изведба/документација/задржување на тест случаи? f. Грешка и справување со проблеми? g. Корекција и ескалација? h. Формално одобрување? 3. Дали тестовите се спроведуваат на системот за производство во живо или во тест средина?		• Планови за тестирање и други документи релевантни за тестирање на голема промена на ИТ апликација/програма

6) КОНТРОЛИ НА АУТСОРСИНГ НА ИТ ИНФРАСТРУКТУРАТА

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни се документи
1.	***Цел на контролата:*** *Идентификување на услугите што ги дава ИТ. Дефинирање, договорање и редовно прегледување на договори на ниво на услуга, кои треба да ги покриваат барањата за поддршка на услугите, поврзаните трошоци, улогите и одговорностите итн., и да бидат изразени во работни услови.* ***Референци за регулаторна рамка:*** *CP чл. 28a(2)(в); IR Arts 22a(1)(d), 48(c,f) и 108; ICS5, ICS8, ICS10, ICS11 и ICS12* ***Критериуми за поврзани информации:*** *доверливост, интегритет, ефикасност и ефективност*	DS1.1	1. Дали постојат јасно дефинирани бенефиции и деловни цели во поддршка на одлуката за аутсорсинг? 2. Дали барањата и очекувањата на раководството се јасно дефинирани во договорот/SLA? 3. Дали ризиците беа оценети при одлучувањето за аутсорсинг и беа земени предвид при специфицирање на потребните контроли? 4. Дали ИТ проектот беше спроведен во согласност со постоечките стандарди за управување со проекти?		• Договор(и) • SLA(и)
		AI 4.1 AI 5.2 DS1.3 DS1.6 DS2.4	5. Дали договорот/SLA јасно ги дефинира безбедносните барања: a. Мрежна безбедност?		

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни се документи
			b. Физичка безбедност? c. Антивирусна заштита? d. Логички контроли за пристап?		
			6. Дали барањата за резервна копија на податоци се јасно дефинирани? 7. Дали се вклучени одредби за постапките за континуитет на работењето? 8. Дали има клаузула за усогласеност со прописите за заштита на личните податоци?		
			9. Дали договорот/SLA дава детален опис на услугата што треба да се обезбеди: a. Барања за хардвер и софтвер? b. Сервисна поддршка (пулт за помош, управување со инциденти, управување со проблеми)?		

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни се документи
			c. Управување со одржување и промени? d. Дали има потреба од екипирањеза ИТ?		
			10. Дали договорот/SLA го вклучува/покрива следново: a. Формално управување и законско одобрување? b. Трошоци, со спецификации за плаќање (вклучувајќи го и периодот)? c. Улогите и одговорностите на раководителите? d. Постапка и зачестеноста на комуникација со корисникот/давателот на услугит? e. Времетраење на договорот? f. Процедури за решавање проблеми? g. Казни за неисполнување?		

	Контролни цели и повикување на регулаторната рамка	COBIT ref.	Тестови на контроли	Евалуација	Потребни се документи
			h. Постапката за распуштање? i. Постапката за измена на договорот? j. Гаранции за необјавување/неоткривање? k. Право на пристап и право на ревизија?		
2.	***Цел на контролата:*** *Континуирано следење на одредени критериуми за перформанси на ниво на услуга. Извештаите за постигнувањата на нивоата на услуги треба да се обезбедат во формат што е разбирлив за засегнатите страни.* ***Референци за регулаторна рамка:*** *IR чл. 22а(1)(д); ICS9 и ICS15* ***Критериуми за поврзани информации:*** *Ефикасност и ефективност*	DS1.5 ME1.4 ME1.5 ME1.6	1. Дали договорот/SLA ги дефинира постапките за известување во однос на видот, содржината, зачестеноста и дистрибуцијата на извештаите? 2. Дали постои процедура за континуиран мониторинг и редовно известување за постигнувањето на целите? 3. Дали се воспоставени формални критериуми за изведба за олеснување и мерење на постигнувањето на целите на SLA?		• Извештаи од мониторинг

ЗАВРШНИ ЗАБЕЛЕШКИ

Ажурирањето на ова упатство е во надлежност на Сектор за централна хармонизација на системот на внатрешна финансиска контрола во јавниот сектор (Централната единица за хармонизација) при Министерството за финансии. Оваа верзија на упатството Централната единица за хармонизација го подготви во соработка со експертите ангажирани во рамки на твининг проектот “Зајакнување на функциите на буџетско планирање, извршување и внатрешна контрола”. Проектот е финансиран од Европската Унија, преку Националната ИПА Програма за 2018 г.

Оваа публикација е изработена со финансиска поддршка на Европската Унија. Нејзината содржина е единствена одговорност на авторот. Изразените ставови нужно не се смета дека го одразуваат официјалното мислење на Европската Унија.