УКАЗАНИЕ 5100

Указание за одит на информационни системи

Указанията на ИНТОСАЙ се изготвят от Международната организация на върховните одитни институции като част от Рамката за професионални становища на ИНТОСАЙ.

За повече информация посетете

www.issai.org

INTOSAI

Този документ е разработен преди учредяването на Рамката за професионални становища на ИНТОСАЙ през 2016 г. Ето защо може да се различава формално от последващи издадени указания на ИНТОСАЙ.

ИНТОСАЙ, 2019 г.

1) Първоначално публикувана версия под името МСВОИ 5100 – „Указания за ИТ одит“, 2016 г.

2) Изменени и преименувани на Указание 5100 – „Указания за одит на информационните системи“, 2019 г.

СЪДЪРЖАНИЕ

1

ВЪВЕДЕНИЕ

1.1 Указание 5100 описва общите положения при одит на информационните системи като част от Рамката за професионални становища на ИНТОСАЙ. Целта е да се осигури основата за развитие на бъдещи указания за одит на информационните системи от серията 5100-5109, част от тази рамка.

1.2 Очертаната в настоящето указание рамка е в съответствие с основните принципи на одита в публичния сектор (МСВОИ 100), основните принципи на финансовия одит (МСВОИ 200), принципите на одита на изпълнението (МСВОИ 300) и принципите на одита за съответствие (МСВОИ 400).

1.3 Върховните одитни институции (ВОИ) имат мандат за одит на правителствените институции и организациите от публичния сектор в съответствие с възложените им правомощия [1]. Посредством дейността си ВОИ целят да стимулират ефикасността, отчетността, ефективността и прозрачността в публичната администрация [2].

1.4 Държавните институции и организациите от публичния сектор въвеждат все по-широко технологичните новости в своите информационни системи, с цел да повишат ефективността и ефикасността на дейността си и да предоставят широк кръг публични услуги. Това е възможно, благодарение на капацитета, осигуряван от информационните технологии, за въвеждане, съхранение, извличане и предоставяне на информация по електронен път, което от своя страна допринася съществено за подобряване на точността, конфиденциалността и своевременното предоставяне на информация от ИС. В допълнение, обществените услуги все по-често се предоставят електронно, в резултат публичната администрация се налага да функционира като цифрова платформа за предоставяне на услуги и инфраструктура за други информационни системи, основаващи се на ИТ.

1.5 Този преход към компютъризирани информационни системи и електронна обработка на данни в одитираните обекти от публичния сектор доведе до съществена промяна в средата на работа на ВОИ. Нарастват публичните разходи за информационни технологии. Необходимо е също да се потвърди, че в организациите от публичния сектор са въведени вътрешни ИТ контроли, които гарантират конфиденциалността, неприкосновеността и наличността на данните. Ето защо за ВОИ е задължително да развият подходящ капацитет за цялостна проверка на контролите, свързани с информационните системи.

1 ИНТОСАЙ -П 1 „Декларация от Лима“

2 Резолюция А/66/209 на Генералната асамблея на ООН

2

ЦЕЛИ НА НАСТОЯЩОТО УКАЗАНИЕ

2.1 МСВОИ 100, 200, 300 и 400 определят основните положения по отношение извършването на финансов одит, одит на изпълнението и одит за съответствие. Те задават общите принципи, процедури, стандарти и очаквания за одитора и са приложими с пълна сила и към одита на информационните системи.

2.2 Целта на настоящите указания е да насочат одитора при осъществяването на одит на изпълнението и/ или за съответствие с фокус върху конкретната специфика на информационните системи или при одитни проверки, където анализът на информационната система е част от по-всеобхватен одитен ангажимент – финансов одит, одит за съответствие или на изпълнението.

2.3 Настоящите указания могат да се използват от одиторите за планиране и осъществяване на одита, за докладване и проследяване изпълнението на препоръките [3].

3 МСВОИ 100

3

ОПРЕДЕЛЕНИЯ

3.1 Информационни системи: комбинация от стратегически, управленски и оперативни дейности за събиране, обработка, съхранение, разпространение и използване на информация и свързаните с това технологии. Информационните системи имат различни мащаби – от обикновена ведомост, в която на ръка се вписват получени и изплатени суми, до комплексна система, базирана на ИТ, напр. система за изчисление на данъците, където всички процеси са автоматизирани – събиране на данни (напр. данъчни декларации, подавани през интернет портал), съхранение на сървъри, изчисление (на базата на програмиран код, използващ правилата за данъчно облагане) и обмен на информация за изискуемите данъци, за възстановяване и потвърждение (в реално време или през определени интервали). Информационните технологии представляват хардуер, софтуер, комуникационно и друго оборудване, използвани за въвеждане, съхранение, обработка, прехвърляне и предоставяне на данни в определен формат.

3.2 Одитът на информационните системи може да бъде определен като преглед на контролите, свързани с информационните системи, основани на ИТ, чиято цел е да се установят отклонения от критериите, зададени на база на вида одитен ангажимент – финансов одит, одит за съответствие, одит на изпълнението.

4

ОБХВАТ

4.1 Настоящите указания могат да бъдат използвани от одиторите за осъществяването на одит на изпълнението и/или за съответствие с фокус върху спецификата на информационните системи, както и за одит на информационните системи като част от по-голям одитен ангажимент – финансов одит, одит за съответствие и/ или на изпълнението.

4.2 Настоящият документ дава допълнителни указания как всяка проверка на информационните системи може да бъде извършена в рамките на финансов одит/ одит на изпълнението/ за съответствие без допълнителни изисквания към осъществяването на одита.

5

ПЛАНИРАНЕ НА ОДИТ НА ИС

5.1 ВОИ могат да въведат планиране на одита на ИС на базата на оценка на риска в съответствие с описания процес в МСВОИ 100, МСВОИ 200 (Финансов одит), МСВОИ 300 (Одит на изпълнението) и МСВОИ 400 (Одит за съответствие) и в зависимост от целите на одитния ангажимент.

5.2 Одитната работа в рамките на проверката на ИС се определя от целите и обхвата на одита. Като примери могат да се посочат:

1) оценка на приложимите общи контроли[4] и контроли на ниво приложения[5], осигуряващи надеждността на данните в информационните системи, което от своя страна има отражение върху финансовите отчети на одитирания обект;

2) предоставяне на увереност относно съответствието на процесите в информационната система със законодателството, политиките и стандартите, приложими за одитирания обект;

3) предоставяне на увереност, че ИТ ресурсите обезпечават постигането на целите на организацията ефикасно и ефективно, както и че приложимите общи контроли и контроли на ниво приложения не допускат, установяват и коригират случаите на разпиляване, разточителство или неефективно използване и управление на информационните системи.

5.3 На базата на оценката на риска обхватът на одита на ИС може да се основава на всяка една или всички долуизброени области[6] :

1) политика на организацията в областта на ИТ [7];

2) организационна структура в областта на ИТ;

3) общи контроли за съответната автоматизирана част от дейността;

4) управление на активите;

---

4 Общите контроли са ръчни или автоматизирани процедури, чиято цел е да се осигури конфиденциалността, целостта и наличността на информацията във физическата среда, в която се разработва, поддържа и експлоатира информационната система.

5 Контролите на ниво приложение представляват ИТ процедури (ръчни или автоматизирани) в рамките на дадена информационна система, които влияят върху обработката на транзакциите и могат да бъдат свързани с валидиране на данните на входа, правилната им обработка и предоставяне на изходните данни, както и с целостта на данните в главния файл (master data).

6 Повечето от описаните области са адаптирани на база на ISO/IEC 27001.

7 вкл. аспекти на стратегическото управление.

5) разработване, придобиване и поддържане на информационните системи, вкл. картографиране на бизнес процесите и свързаната с това логика на програмиране;

6) управление на ИТ операциите;

7) управление на физическата среда;

8) управление на човешките ресурси;

9) управление на комуникациите;

10) управление на информационната сигурност [8];

11) управление на законосъобразността;

12) управление на непрекъсваемостта на дейността и възстановяване на системата след срив;

13) управление на контролите на ниво приложение.

5.4 ВОИ избира периода, който да бъде обхванат от одитния анализ (напр. 1 година, 3 години и т.н.) при определяне на обхвата на одита на ИС. Той следва да съответства на целта на одита.

5.5 Когато одита на ИС е част от по-всеобхватен одитен ангажимент, ВОИ гарантира интегрираната работа на одитния екип, така че да се постигне общата цел на одита. За осигуряването на ефективна интеграция, ВОИ може да изиска:

1) всеобхватно документиране на работата, която се извършва от одиторите на ИС;

2) въвеждане на протокол за споделяне на информация между одиторите на ИС и техните колеги;

3) определяне кои информационни системи и цели на контрола влизат в обхвата на одита.

5.6 ВОИ осигурява необходимите членове за одитния екип, които притежават капацитет за извършването на одит на ИС, така че да бъдат постигнати желаните цели на одита.

5.7 Необходимите знания, умения и квалификации могат да бъдат осигурени чрез обучение, наемане и ангажиране на външни консултанти в съответствие със стратегическия план на ВОИ.

5.8 ВОИ гарантира, че екипите за одит на ИС:

1) имат капацитет да анализират техническите елементи на ИТ-базираната информационна система, вкл. всички използвани приложения, така че да могат да оценят ИТ инфраструктурата за целите на одита;

8 вкл. кибер сигурност

2) разбират правилата, регулациите и средата, в която функционира ИТ-базираната информационна система на одитирания обект;

3) имат познания за картографирането на бизнес процесите в програмната логика на одитирания обект;

4) прилагат както стопански, така и ИТ познания, за да оценят риска от ръчно управление на системна програма или конфигурация, което би позволило изключения при обработка на транзакции;

5) имат капацитет да оценят дизайна и да тестват оперативната ефективност на контролите на ниво приложение в съответните информационни системи;

6) познават одитната методика, вкл. приложимите за съответната ВОИ одитни стандарти и указания;

7) разбират критериите за изпълнение/ съответствие в областта на ИТ, на базата на които се оформят одитните констатации, вкл. рамките за управление на ИС като COBIT, ITIL, TOGAF;

8) владеят техниките за събиране на одитни доказателства от автоматизирани системи;

9) познават способите за одит на ИС, които се прилагат за събиране, анализиране и възпроизвеждане на резултатите от подобен анализ или повторно изпълнение на одитираните дейности;

10) могат да достъпват и използват ИС инфраструктурата с цел събиране и запазване на доказателства;

11) могат да достъпват и използват средствата за ИС одит, за да събират и анализират доказателства.

5.9 ВОИ могат да приложат различни подходи за разпределяне на своите човешки ресурси за извършване на одит на ИС. Може да се сформира централен отдел от ИТ специалисти, които да подпомагат одитните екипи на ВОИ при провеждането на такива одити или ИТ специалисти да се разпределят по екипите при необходимост. С увеличаването на одитите на информационни системи ВОИ могат да помислят за създаването на нарочно звено или отдел за ИТ одит, на който да се възложи осъществяването на всички одити на ИС и който да си взаимодейства с другите екипи на институцията, запознали се с дейността на одитирания обект през годините, така че ИТ одиторите бързо да попълнят своите знания за функциите и процесите в обекта. С все по-дълбокото навлизане на технологиите в информационните системи ВОИ следва да гарантират, че всички техни одитори притежават подходящи способности за одит на ИС.

5.10 ВОИ могат да привличат външни ресурси като ИТ консултанти, подизпълнители, специалисти и експерти за целите на своите ИС одити,

когато не притежават служители със съответните квалификации. Одитните институции следят те да бъдат обучени и запознати по подходящ начин с указанията за професионално поведение, процесите и продуктите на ИТ одита, приложими в съответната ВОИ, и осъществяват адекватен мониторинг на работата на външните консултанти на базата на подписан договор или споразумение за ниво на техническо обслужване, както и чрез адекватно участие на служителите на ВОИ в планирането и изпълнението на одита, докладването и проследяването на препоръките. Следователно ВОИ трябва да разполага с добре обучени служители, които да осъществяват мониторинг на работата на външните изпълнители и да следят за спазване на указанията и споразуменията за ниво на техническо обслужване.

5.11 За оценката на риска във връзка с одита на ИС могат да се приложат подходите, предвидени в МСВОИ 100, 200, 300 и 400, в допълнение към принципите, касаещи специфичните одити на ИС, очертани по-долу:

1) Присъщ риск - вероятността определени характеристики на ИТ-базираната информационна система по своята същност да водят до негативно въздействие върху изпълнението на функциите на одитирания обект. Напр. присъщ риск за дадена информационна система на одитирания обект, която има за цел да предоставя информация на обществото, е след достигане на определен таван от потребителски заявки, системата да блокира и да не предостави желаната информация на гражданите. Одитираният обект може да въведе контроли за смекчаване на присъщия риск, но в много случаи просто трябва да се примири с наличието му и да го ограничи до приемливо ниво. Присъщият риск може да бъде оценен преди действието на контролите или одиторите да вземат предвид риска от неразкриване.

2) Контролният риск за ИС се свежда до вероятността въведените от одитирания обект ИТ контроли да не успеят да смекчат негативното въздействие, което целят да ограничат. Например в информационната система на одитирания обект, която трябва да гарантира ограничен достъп до конфиденциална информация единствено за оторизираните лица, може да се въведе контрола под формата на изискване за представянето на потребителско име и парола за вход. Тук контролният риск се състои в това потребителското име и парола да не са достатъчно сигурни и да могат да бъдат възпроизведени от неоторизирани служители след неколкократни опити, което би довело до разкриване на конфиденциална информация и потенциален негативен ефект за одитирания обект. Ако организацията изисква да бъдат използвани сигурни и комплексни пароли, съдържащи комбинация от различни азбуки, числа и специални символи и информационната й система

не допускат повече от „N“ на брой опити за въвеждане на парола за даден потребителски профил, тя би имала по-нисък контролен риск в сравнение с организации, в които подобни практики не се прилагат.

3) Рискът от неразкирване представлява вероятността одиторът да не успее да установи отсъствието, неуспешното действие или неадекватността на ИТ контролите, въведени от одитирания обект, което би имало негативно въздействие за обекта.

5.12 За осъществяването на базирана на риска оценка на ИТ системите ВОИ може да подбере подходяща за своите цели методика. Тя може да варира от обикновена класификация на рисковия профил на ИТ средата в одитирания обект като висок, среден или нисък, която се базира на знанията на ВОИ за съответния обект и неговата среда и на професионалната преценка на одитния екип, а може да се основава и на по-сложни изчисления за задаване цифрова стойност на риска на базата на обективни данни, събрани за одитирания обект[9] .

5.13 Прагът на същественост на даден одитен въпрос, свързан с ИС, може да бъде определен в съответствие с общата рамка за същественост на ВОИ. Разбирането за същественост може да варира в зависимост от характера на одитния ангажимент в областта на ИС. Прагът на същественост за финансовите одити, одити за съответствие и на изпълнението, на които се базира одита на ИС, се определя според принципите, залегнали в МСВОИ 100, 200, 300 и 400[10].

9 Наръчник по одит на информационните технологии за върховни одитни институции, изготвен от Работната група на ИНТОСАЙ по ИТ одит / Инициатива за развитие на ИНТОСАЙ

10 МСВОИ 200 - Принципи на финансовия одит, МСВОИ 300 – Принципи на одитна на изпълнението, МСВОИ 400 – Принципи на одита за съответствие

6

ИЗВЪРШВАНЕ НА ОДИТА

6.1 ВОИ осъществяват одити на информационни системи, като следват описаните процеси в МСВОИ 200 – „Финансов одит“, МСВОИ 300 – „Одит на изпълнението“ и МСВОИ 400 – „Одит за съответствие“ в зависимост от характера на конкретния одитен ангажимент.

6.2 Конкретно за одита на информационните системи одиторите могат да потърсят необходимото съдействие и подкрепа от страна на одитирания обект, вкл. достъп до записи и информация. След съгласуване с одитирания обект одиторите могат да определят режим на достъп до електронни данни във формат, който би позволил анализ. Този начин на достъп е конкретен за всяка ВОИ.

6.3 Преди да започне оценката на контролите за дадена информационна система, одиторът се запознава с нейната архитектура и основните данни и източници, с цел да определи какви одитни похвати и техники ще приложи.

6.4 При получаване на голям пакет от данни, т.нар. „data dumps“[11] от одитирания обект одиторът изисква всеки набор от данни да бъде придружен с писмо от одитирания обект, в което се уточнява:

1) източникът на данните (посредством посочване на идентификатор за времето /time stamp/, в което е генериран наборът от данни/ или неговата хеш-сума), за да се гарантира целостта на данните, тяхната автентичност [12] и неопровержимост[13]

2) параметрите на приложения подход за извличане на данните от изпратения пакет, т.е. използвани търсения/ генерирани справки;

3) ако одиторът не получи подобно придружително писмо от одитирания обект, той може да генерира вътрешен документ, в който отбелязва датата, на която са получени данните, от кой файл е извлечен пакетът от данни и дали те произхождат от производствената или друга среда и т.н.

6.5 Одиторът оценява въведените от одитирания обект ИТ контроли (общи и на ниво приложение), за да определи доколко са надеждни и достатъчни. Тази оценка може да се извърши чрез подходяща

11 „data dump” – голям пакет от данни, прехвърлени от една система или локация към друга.

12 Проверка за автентичност (authentication) – действие по потвърждаване идентичността на даден потребител – Речник на термините, ISACA

13 Неопровержимост (non-repudiation) - гаранция, че дадена страна не може да отрече на по-късен етап изпращането данните; доказателство за целостта и произхода на данните, което може да бъде потвърдено и от трета страна - Речник на термините, ISACA

комбинация от следните техники: събеседване, въпросници, наблюдение, проследяване, графики на процесите, извличане и анализ на данни, потвърждение, повторно изчисление, повторна обработка и потвърждение от трети страни. Обхватът на оценката на ИТ контролите може да включи проверка дали в одитирания обект са въведени:

1) политика за ИС, с която служителите са запознати;

2) структура за управление на ИС, която функционира добре;

3) правила за периодична инвентаризация на активите от ИС и дали са установени нужди от разширяване, подмяна или премахване;

4) процеси за споделяне на инфраструктура и общи услуги за ИС с други организации от публичния сектор;

5) процес за разработване, придобиване и поддържане на информационни системи (вкл. управление на промяната) и дали персоналът е запознат с него;

6) процеси за ИТ операциите (вътрешно изпълнение, възлагане на подизпълнител, споразумения за обслужване), които са доведени до знанието на съответните лица;

7) мерки за гарантиране на физическата сигурност и адекватна физическа работна среда;

8) мерки за обучение и запознаване на персонала с въпросите, свързани с конфиденциалността, ненарушимостта и наличността на информацията, както и дали са въведени изисквания за спазване на политиката и структурата за управление на ИС;

9) мерки за гарантиране конфиденциалността, целостта и наличността при различните начини и канали за комуникация;

10) мерки за управление на информационната сигурност;

11) мерки, гарантиращи спазване на законодателството;

12) мерки за гарантиране непрекъсваемост на дейността и възстановяване след срив;

13) подходящи и надеждни контроли на ниво приложение за всяка информационна система. При тази оценка може да се идентифицират съществените елементи от приложенията, критичните за одитирания обект приложения, да се направи преглед на наличната документация, събеседване с персонала, запознаване с контролните рискове на ниво приложения и тяхното въздействие за одитирания обект, както и да се разработят проверки за адекватността и надеждността на контролите на ниво приложение.

6.6 Ето защо при оценката на общите контроли и тези на ниво приложение може да се обхванат политиките на одитирания обект, процесите, човешките ресурси и системите в съответствие с целите на

одита на ИС.

6.7 В зависимост от целта на одита одиторите се фокусират върху разработването, прилагането и оперативната ефективност на контролите. Когато фокусът е върху разработването на контролите, е достатъчно да се проведе събеседване или проверка на документираните правила за дейността. При фокус върху прилагането на контролите допитването може да се окаже недостатъчно и да се наложи прилагането на проследяващи тестове или анализ на данни, за да се потвърди, че разработената контрола се прилага на практика. И накрая, ако одиторът иска да провери оперативната ефективност на контролите, може да му се наложи да тества извадка от транзакции, за да покаже, че контролният механизъм е работил ефективно през одитирания период.

6.8 Одиторите могат също да разгледат как доказателствата, касаещи общите контроли оказват въздействие върху естеството, времетраенето и обхвата на доказателствата, необходими за придобиване на увереност за състоянието на контролите на ниво приложение. Ако одиторът е събрал достатъчно уместни одитни доказателства относно ефективността на общите контроли за логически достъп на служителите до ИТ системите и управлението на промяната в производствена среда, той може да направи своето заключение относно оперативната ефективност на автоматизираните контролни процедури. За тази цел могат да се проверят по-малка извадка от транзакции, тъй като ефективността на общата ИТ среда осигурява доказателства на одитора относно ефективността на контролите на ниво приложение за проверявания период. При ръчно прилагани контроли на ниво приложение може да се наложи одиторът да анализира извадка с подходящ размер според избраното ниво на увереност.

6.9 На база на оценката на ИТ контролите одиторите могат да идентифицират приоритетни области за директни съществени проверки, които включват подробни тестове на ИТ контролите чрез използване на различни компютърно-базирани одитни техники (CAATs) за търсене, извличане и анализ на данни. Одиторите могат да разработят и изпълнят директни съществени проверки, за да подкрепят одитните цели. На база на изискванията си одиторите могат да подберат подходящи компютърни одитни техники.

6.10 С помощта на CAATs одиторите могат да приложат техники за ИС одит като анализ на записите за вход в системата, доклади за изключения, сумиране на полета (field wise totaling), съпоставка на файлове, стратифициране, формиране на извадки, проверки за дублиране, проверка за възраст на данните, изчисление на виртуални полета и т.н. Предимствата на използването на компютърно-базираните одитни техники включват възможности за анализ на големи по обем данни, повторяемост на тестовете за

отделните пакети от данни и с различни критерии, както и автоматизирано документиране на одитните проверки и предоставяне на резултати, придружени с времеви печат.

6.11 Одиторите не винаги имат възможност да проверят всички събития, транзакции, модули или ИТ системи, предвид ресурсните ограничения и разумното съотношение между разходи и ползи. При подобни ситуации на база на приетия праг на същественост ВОИ може да въведе принципа на подробна проверка на одитни извадки, с цел да се изведат разумни одитни заключения. ВОИ може да използва различни компютърно-базирани одитни техники за работа на извадков принцип и за определяне на подходящия размер на извадката в зависимост от съответните присъщ и контролен риск. Одитните извадки[14] се формират с цел одиторът да получи разумна база, върху която да изгради своите изводи относно цялата съвкупност от данни, като се позове на заключенията от прилагането на одитни процедури и анализ на одитната извадка. Одиторът взима предвид предназначението на одитната процедура и характеристиките на съвкупността, за да определи достатъчен размер на извадката, така че рискът, свързан с работата на извадков принцип, да бъде сведен до приемливо ниво. Когато одитът се извършва в ИТ среда, това може да позволи анализ на 100% от съвкупността, особено на етап предварителна оценка. За целите на директните съществени проверки обаче, може да се наложи да се използват извадки. При формирането на извадки в рамките на финансов одит одиторът прилага МСВОИ 2530 [15].

6.12 Одиторите гарантират, че събраните и документирани електронни доказателства са достатъчни, надеждни, точни и подкрепят одитните наблюдения. Електронните доказателства могат да бъдат под формата на файлове с данни, записи (log) на потребители, аналитични модели, отчети от управленски информационни системи и т.н. и следва да са събрани и съхранени по подходящ начин, така че да бъдат налични за предоставянето на увереност относно точността и валидността на одитния процес. Събраните доказателства в рамките на одита на ИС трябва да съдържат необходимите идентификатори за време и подробности относно стъпките в анализа на данни, така че да има яснота относно това кога съответното доказателство е създадено, съхранено и последно променено, за да се намали риска от последващи промени.

6.13 Одитната документация трябва да бъде съхранена и защитена от всякакви модификации и неоторизирано заличаване. ВОИ могат да разработят нови стандарти за съхранение на документацията от одита на ИС или да адаптират съществуващите такива от общ характер. Така определеният изискуем период на съхранение трябва да е съобразен със съответния мандат на ВОИ и правилата за дейността ѝ. Следва да се обърне особено внимание на носителите, формàта и очакваната продължителност на живота им, както и на изискванията за съхранение,

14 МСВОИ 2530, Финансов одит, Одитна извадка, раздели 6 до 9.

15 МСВОИ 2530, Финансов одит, Одитна извадка, раздели 6 до 9.

така че данните да останат четими в рамките на задължителния период в съответствие с политиката за архивиране на ВОИ. Това може да наложи необходимостта от конвертиране на данните в различен формат, за да се вземе предвид развитието на технологиите.

6.14 При запознаване с технически доклади, изготвени от трети страни по специфични технологични теми, одиторите могат да приложат подходящи процедури, на базата на които да се уверят относно аспектите в тези доклади, касаещи финансите, съответствието или изпълнението[16] . Ако в резултат от подобни процедури одиторът реши да се позове на съответния доклад, това следва да бъде надлежно оповестено.

6.15 МСВОИ предвиждат, че одиторите следва да установят ефективна комуникация през целия одитен процес и да информират одитирания обект относно всички свързани с одита въпроси (МСВОИ 100, параграф 43). При одити, които обхващат проверка на ИС, резултатите от работата на ИТ одитора понякога се предоставят на одитирания обект в отделно писмо. В такива случаи е важно да се разясни как резултатите от одитната работа по ИС се съотнасят към останалата информация, подадена до одитирания обект в рамките на съответния финансов одит, одит на изпълнението или за съответствие и как касаещите ИС резултати ще намерят отражение в одитния доклад на ВОИ.

16 Когато проверката е в рамките на финансов одит, одиторът може да приложи МСВОИ 2402 – Одитни съображения във връзка с предприятия, които използват подизпълнители

7

ОДИТЕН ДОКЛАД

7.1 Тъй като съответният одитен ангажимент на ВОИ за проверка на ИС обикновено се осъществява в рамките на финансов одит (МСВОИ 200), одит на изпълнението (МСВОИ 300) или одит за съответствие (МСВОИ 400), одиторите се придържат към изискванията за докладване, съдържащи се в съответните стандарти. Те са специфични за всяка ВОИ. Одитната институция може също да залага конкретни прагове на докладване въз основа на същественост на своите констатации. В допълнение, при докладване относно извършения одит на ИС одиторът взима предвид законовите и вътрешни ограничения, касаещи оповестяването на финансова и техническа информация.

7.2 Одиторът трябва да има предвид необходимостта от ограничено използване на технически жаргон, както и чувствителния характер на представената в доклада информация (напр. пароли, потребителски имена, идентификация и лични данни). Независимо от техническите характеристики на одита на ИС, одиторът трябва да изготви доклада си така, че той да бъде лесно разбираем за висшето ръководство на одитирания обект, заинтересованите страни и обществеността. В доклада може да се включи подробен речник на термините с препратки към определенията на съкращенията и термините и примери как съответният процес действа в контролирана среда.

7.3 Одиторите трябва да имат предвид потенциалния негативен ефект от одитния доклад за ИС след неговото публикуване. Например, ако в одитния доклад са описани рискове за сигурността на информационната система в одитирания обект и той бъде оповестен преди въвеждането на необходимите контроли за смекчаване на рисковете, това ще доведе до широкото разпространение на информация относно уязвимостта на информационната система. При подобни ситуации одиторите могат да помислят за забавяне публикуването на доклада си до въвеждането на необходимите контроли или избягване на подробно докладване по конкретните рискове за сигурността, за да не се допусне потенциален негативен ефект за одитирания обект.

8

ПРОСЛЕДЯВАНЕ ИЗПЪЛНЕНИЕТО НА ОДИТНИТЕ ПРЕПОРЪКИ

8.1 Тъй като одитните ангажименти за проверка на ИС се осъществяват в рамките на един или няколко от основните видове одит, одиторите следва да разглеждат изискванията за проследяване на препоръките от подобни ангажименти наравно с тези от финансовия одит (МСВОИ 200), одита на изпълнението (МСВОИ 300) и одита за съответствие (МСВОИ 400).