УКАЗАНИЕ 5259

Информационни системи за публичния дълг

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.

INTOSAI

ИНТОСАЙ, 2019 г.

1. **Приети като МСВОИ 5450 – Ръководство за одит на информационните системи за управление на публичния дълг през 2016 г.**

2. **След учредяването на Рамката за професионални становища на ИНТОСАЙ документът е преименуван на Указание 5259 – Информационни системи за публичния дълг с редакционни поправки от 2019 г.**

СЪДЪРЖАНИЕ

ПРЕДГОВОР

Публичният дълг стои в центъра на всяка дискусия относно управлението на публичните финанси. В стремежа си за разширяване на икономиките и подобряване на социалните услуги в своите държави, повечето правителства изпитват големи финансови потребности. На теория, публичният дълг представлява ефективен инструмент за икономически растеж и за равномерно разпределение на данъчната тежест между настоящите и бъдещите поколения от данъкоплатци. Но поради значимостта му за икономическото салдо, изключително важно е държавният дълг да се измерва и управлява с голямо внимание.

Основната цел на управлението на дълга е да се осигури стабилно финансиране на възможно най-ниска цена и на разумни нива на риска с цел осъществяване на правителствените дейности. Преработените насоки за управление на държавния дълг на Световната банка и Международния валутен фонд (МВФ) предоставят набор от стабилни практики по отношение на вътрешните контроли за управление на дълга. Сред тях е и определението, че „дейностите по управление на дълга следва да бъдат подкрепени от точна и всеобхватна управленска информационна система с подходящи защити". Държавите, които искат да гарантират ефективно управление на държавния дълг, трябва да си поставят за приоритет развиването на надеждни системи за регистриране и докладване на дългова информация. Необходимо е не само да разработят данни относно дълга и да се осигурят навременните плащания във връзка с обслужването на дълга, но също и да се подобри качеството на отчитането на бюджета и прозрачността на публичните финансови сметки, което дава възможност на лицата, които разработват политиките и тези, които управляват дълга да постигат целите относно държавния дълг.

Одитът на информационните системи за управление на публичния дълг се стреми да гарантира ефективността и ефикасността на управлението на държавния дълг. По тази причина, всеки подобен одит следва да бъде определен като одит на изпълнението. Въпреки това, уместно е тази одитна работа да се разглежда и в контекста

на финансовите одити, чийто акцент е върху установяване дали финансовата информация, която подава правителството е в съответствие с нормативната рамка, приложима към представянето на финансовите отчети, както и дали информацията е надеждна, без измами и грешки. В този контекст, тази работа придобива голяма значимост, тъй като има принос за установяване на информационна система, която събира и генерира точна и надеждна информация за един от най-важните елементи на държавните финанси – държавния дълг.

Настоящото Указание предоставя на одиторите насоки относно извършването на одит на информационните системи за управление на държавния дълг. Тъй като Международната организация на Върховните одитни институции (ИНТОСАЙ) вече разполага с документи относно одити на информационните технологии (ИТ), разработени от Работната група по ИТ одити (РГОИТ), настоящото Указание се концентрира върху контролите на приложенията, които следва да бъдат специфични за информационните системи за управление на държавния дълг.

СПИСЪК НА СЪКРАЩЕНИЯТА

ПНД – планиране на непрекъснатостта на дейността

CAAT – компютърни техники за одит

CS-DRMS – Система на Секретариата на Британската общност за записване и управление на дълга

СУДФА – Система за управление на дълга и финансови анализи

СУД – Служба за управление на дълга

ПВБ – план за възстановяване при бедствия

ИСУФ – Информационна система за управление на финансите

МВФ – Международен валутен фонд

ИНТОСАЙ – Международна организация на Върховните одитни институции

ИТ – информационни технологии

ИСУПД – информационна система за управление на публичния дълг

ВОИ – Върховна одитна институция

СИД – Интегрирана система на федералното правителство на Бразилия относно дълга

УНКТАД – Конференция на ООН за търговия и развитие

РГОИТ – Работна група по одит на ИТ

РГОПД – Работна група по публичния дълг

Съгласно заданието, разработено от Управителния съвет на ИНТОСАЙ, на Работната група по одит на публичния дълг (РГОПД) е възложено да публикува указания и други информационни материали, които върховните одитни институции (ВОИ) да ползват за насърчаване на правилното докладване и доброто управление на държавния дълг.

Настоящото Указанив повишава капацитета на РГОПД за осигуряване на обща рамка, която да се използва в одити на ВОИ за оценка на общите контроли и контролите на приложенията на информационните системи за управление на публичния дълг (ИСУПД). Важно е да се обърне внимание, че в заданието, ИСУПД включва една или повече информационни системи, използвани за управление на публичния дълг.

С напредъка в областта на ИТ, държавните организации все повече зависят от използването на ИТ за извършване на своите дейности и предоставяне на услуги, както и за обработка, поддръжка и докладване на основна информация. Съгласно Работния документ на МВФ, „ИСУФ (Информационна система за управление на финансите) най-общо се отнася до компютризацията на процеса на управление на публичните разходи, в това число формулиране, изпълнение и отчитане на бюджета с помощта на напълно интегрирана система за финансово управление на ресорните министерства и другите разходни организации.”

Стандарт 1471 на Института на инженерите по електрически и електронни системи дефинира системите като „набор от компоненти, организирани така че да изпълняват конкретна функция или група от функции.” По-конкретно, основната дейност на дадена система в служба по дълга е да поддържа кредитната база с данни относно заемите на публичния сектор като използва софтуер, който адекватно изпълнява работата по записване и изпълняване на аналитичните функции на службата за управление на дълга (СУД).

ИТ одитите могат да бъдат класифицирани във връзка с преобладаващите подходи по следния начин:

- Управление на ИТ;
- Одит на данни;

- Одит на информационни системи;
- Договаряне във връзка с ИТ, и
- Информационна сигурност.

Най-общо казано, ИТ одиторът прилага повече от един подход; обаче одиторът може да избере преобладаващ подход. В настоящото Указание преобладаващият подход е одит на информационни системи.

Указанието е разделено на три раздела: планиране, оценка на общите контроли и оценка на контролите на приложенията.

1. ПЛАНИРАНЕ

ИСУПД може да бъде разгледана като набор от взаимнозависими части (физически структури, персонал и технологични инструменти), които си взаимодействат с цел записване, контролиране, оценка и управление на транзакции, които се извършват при набиране, поддръжка и клиринг на публичния дълг.

Този етап помага на одитора да вникне в свързаните операции и контроли на системата и свързаните рискове по отношение на присъщите за публичния дълг рискове в оперативния поток. На базата на това одиторът прави оценка на цялостната контролна среда, идентифицира системите, които се използват в управлението на публичния дълг, проучва цялата документация, която се отнася до тези системи и извършва предварителна оценка на риска. Резултатът от оценката ще определи обхвата на процедурите, които ще се използват в етапа на тестване.

ВОИ прави също и проверка на всички структури, отнасящи се до службата по публичен дълг, като персонал, процеси, видове дълг, сигурност на данните, технологични инструменти и други.

На този етап одиторът следва да включи предварителна оценка на структурата и оперативния поток на службата по публичния дълг, като обърне внимание на следното:

- Как е организирана ИСУПД: какви системи се използват за записване, обработване, докладване, контролиране и управление на публичния дълг и кои са основните процеси и функции, извършвани от всяка от системите;
- Функционирането на вътрешния одит;
- Резултати от предишни одити (вътрешни или външни) на ИСУПД;
- Физическо съхранение на документите от операциите;

- Използването на компютърен хардуер и софтуер и отговорността за поддръжката им;

- Операциите, които се обработват от информационните системи и

съответната им значимост;

- Връзката между компонентите на информацията относно публичния дълг;

- Методи и процедури за прилагане на нови или ревизия на съществуващи процедури;

- Предишни оценки на вътрешните контроли на СУД. В случай, че вътрешните контроли на СУД не са били оценявани до момента, ВОИ следва да извърши тази оценка. Това е много важна процедура за оценка на степента на съществуващите рискове, а оттам и за определяне на необходимите одитни тестове.

Равнището на сложност на системата няма значение за оценката на общите контроли, която следва да бъде извършена във всички случаи. Тя определя одитните процедури, които ще се извършват и показва колко ИТ специалисти са необходими за осъществяване на одитната работа. Препоръчително е да има поне един ИТ специалист в екипа, който да извърши работата, отнасяща се до системите. За одиторите в екипа, за които извършването на ИТ одит е новост, е важно да придобият знания относно широко използваните термини. В този случай си струва ВОИ да инвестира в добър технически речник в областта на информационните технологии. Полезен в този смисъл е документът на РГОИТ „Одит на информационни системи – речник на термините". От полза могат да бъдат и някои онлайн речници: вж. напр. http://www.webopedia.com или http://whatis.techtarget.com.

Одиторите, които са запознати с ИТ терминологията трябва също да познават и терминологията, използвана от СУД, особено акронимите и съкращенията (видове заглавия, сектори на СУД, кредитори, наименования на системите, софтуер ползван от СУД и т.н.). Изключително важно е тези знания да са усвоени преди провеждането на интервюта. Полезен речник, разработен от Конференцията на ООН за търговия и развитие (УНКТАД) може да намерите на следните интернет връзки:

- http://unctad.org/en/Docs/pogiddmfasm3r3.en.pdf – Речник на понятията в областта на дълга и СУДФА (версия на английски език)

- http://www.unctad.org/sp/docs//pogiddmfasm3r3.sp.pdf– Glosario de la deuda y del SIGADE (версия на испански език)

За да може да се разбере ИСУПД в детайли, трябва да се познават присъщите информационни (данни) и оперативни потоци. Следователно на етапа на планирането е много важно да се изготви карта на основните

процеси относно публичния дълг (записване, обработване, контрол, сигурност, докладване и анализ), както и да се разбира как се извършват тези процеси посредством информационната система. След това е необходимо да се проведе оценка на риска за идентифициране на по-големите рискове, свързани с основните оперативни и управленски процеси по отношение на публичния дълг, като се има предвид тяхното въздействие и вероятност от появата им. Оценката на риска е решаваща за определяне на обхвата на процедурите, необходими за управление на свързаните нива на риск. Бившият вече МСВОИ 5410, Указания за планиране и извършване на одит на вътрешните контроли относно публичния дълг предоставя указания относно провеждането на оценка на риска. В допълнение, оценката на риска може да бъде поставена в контекста на финансовите одити.

Потоците в ИСУПД почти винаги се уреждат в СУД. Други служби също би могло да отговарят за въвеждането на данни относно дълга, например в случай на договорни дългови задължения. Когато СУД се състои от „бек офис", междинен офис и „фронт офис", всяка основна функция работи със собствен поток от данни и информация. Обикновено фронт офиса отговаря за извършване на транзакциите на финансовите пазари, в това число управление на аукциони и други форми на заеми, както и всички други операции по финансиране. Бек офисът се занимава с приключване на транзакциите и поддържането на финансови регистри. Отделен офис – междинен или по управление на риска, обикновено извършва анализ на риска и мониторинг и докладва рисковете, свързани с портфейла, както и оценява ефективността на лицата управляващи дълга спрямо стратегическите цели/референтните показатели. Основната част от потоците от данни, свързани с публичния дълг, в това число и външните данни, протичат в бек офиса, който е натоварен със записване и контролиране на въведените данни.

При положение, че много държави използват готови системи, които се предлагат на пазара и които са разработени и актуализирани от трети страни/международни организации (напр. Система за управление на дълга и финансови анализи (СУДФА) или Система на Секретариата на Британската общност за записване и управление на дълга (CS-DRMS) за управление на публичния дълг, използването на доклади за изпълнението, напр. искания за системна поддръжка и записи на инциденти, е изключително важно.

При програмата СУДФА, разработена от УНКТАД, ударението пада върху дейностите „надолу по веригата". Тези дейности включват: управление на базите с данни относно дълга, валидиране на данни относно дълга, дългови операции, вътрешно и външно докладване относно дълга, статистика за дълга и базов анализ на дълга, както и изграждане на системни връзки между софтуера за управление на дълга и софтуера за другите финансови дейности. Те допълват дейностите „нагоре по веригата", като анализ на устойчивостта на дълга, който се извършва от други организации, напр. Световната банка. В допълнение, програмата все повече помага на страните да установят връзки между СУДФА за

управление на дълга и друг правителствен софтуер (напр. софтуер, който се използва при изготвянето на бюджета, управление на кешовите наличности и на държавната помощ), или вътре в сложни, интегрирани системи за финансово управление, като елемент на цялостната дейност на дадена страна за управление на финансите. За допълнителна информация вижте: http://unctad.org/dmfas.

Приложението CS-DRMS, което се предоставя от Секретариата на Британската общност, подпомага ВОИ при цялостното записване, управление и анализиране на дълга. Осигурява централизирано „хранилище" на няколко категории държавно или частно секюритизиран външен или вътрешен дълг, включително и краткосрочен дълг. Системата борави също и с безвъзмездната помощ, държавното кредитиране и преотдаване на кредити. За допълнителна информация вижте: http://www.csdrms.org.

Когато имаме държави, които използват СУДФА или CS-DRMS в управлението на публичния дълг, докладите от одити на ИСУПД, извършени от други държави (други ВОИ) могат да бъдат полезни за идентифициране на най-често срещаните недостатъци, на тези които имат най-голямо отражение, или и двете.

Приложение I съдържа таблица във връзка с изискуемата информация, процедури и въпроси на които ВОИ да отговори и което може да се използва от одитния екип на етапа на планирането на работата по одита на системите относно публичния дълг.

2. ОБЩИ КОНТРОЛИ

Общите контроли представляват рамката на цялостния контрол върху ИТ функциите. Тези контроли са разработени за справяне с проблеми, свързани с разработването, операциите и поддръжката на средата. Задачите на общите контроли са да опазват данните, да защитават програмните приложения и да обезпечат непрекъснатата работа на компютрите в случай на неочаквано прекъсване.

Въпреки че одитът на системите относно публичния дълг изисква верификация на общите ИТ контроли, настоящият документ не се спира подробно на тези контроли, тъй като ИНТОСАЙ вече е публикувал документи относно ИТ одити, в които подробно се засяга въпроса за общите контроли.

Препоръчва се при извършване на одит на система, одитният екип да използва вече бившия МСВОИ 5310 , Указания за одити на сигурността на информационните системи (ISec), който дава насоки относно прегледа на сигурността на информационните системи на правителствените организации.

Друг документ, който също може да бъде полезен при планирането на общите контроли е изданието на РГОИТ „Наръчник за изпълнението на ИТ одити за Върховни одитни институции", където е представена основна информация и са засегнати ключови въпроси във връзка с ефективното планиране на ИТ одити.

В Приложение II може да се разгледа матрица за тестванията с някои общи контроли и предложения за процедури на тестване, която да подпомогне одитора при тестване на общите контроли.

Всеобхватният набор от различните категории общи контроли включва описаните по-долу елементи.

» ОРГАНИЗАЦИОННИ КОНТРОЛИ

Организационни контроли са политиките, процедурите и организационната рамка, установени с цел обезпечаване на стабилни политики за човешките ресурси и управленските практики, разделение на задълженията и политики за сигурност на информацията, както и за осигуряване на методи за оценка на ефективността и гарантиране на оперативните контроли и ефикасността.

» КОНТРОЛИ НА ФИЗИЧЕСКИЯ ДОСТЪП

Контролите на физическия достъп включват правила и практики за предотвратяване на неразрешен достъп и намеса в ИТ услугите, в това число административните процедури, като изискване от персонала да удостоверява самоличността си чрез баджове и контрол на посетителите, както и физически мерки като електронни ключалки и врати, камери и други способи за ограничаване на физическия достъп до сървъри и други елементи на критичната инфраструктура.

» КОНТРОЛИ НА ЛОГИЧЕСКИЯ ДОСТЪП

Контролите на логическия достъп използват системата за сигурност, вградена в компютърните системи за предотвратяване на неразрешен достъп до файлове и данни, съдържащи поверителна информация, както и за гарантиране, че всички потребители притежават права за достъп, които се ограничават до изискванията, произтичащи от длъжностната им характеристика. Тези контроли включват защитни стени, антивирусен софтуер и разкриване на проникване и зловреден софтуер.

При модерните системи тези контроли се получават по множество и най-разнообразни начини. Те се внедряват чрез приложен софтуер, оперативна система, система за управление на базата данни, софтуер за контрол на достъпа, мониторинг на обработването на онлайн

транзакциите, мрежата, локалната мрежа и вероятно и друг софтуер.

» КОНТРОЛИ НА ОКОЛНАТА СРЕДА

Контролите на средата са правила, практики и вградени условия за предотвратяване на вреди, причинени от нестабилност на електрозахранването, пожар, прах, вода, храна, екстремни температури, влажност или статично електричество.

Въпреки че акцентът при тези контроли пада върху центъра, където са данните (или зоната отделена за ИТ оборудването, която поставя специфични изисквания към заобикалящата я среда, или най-малкото защита от кражба), те са приложими и към средата, заобикаляща цялото офисно пространство.

» КОНТРОЛИ НА СМЯНАТА НА ПРОГРАМИ

Контролите на смяната на програми включват правила, които гарантират, че всички промени в конфигурацията на системата са извършени по правилния начин, цялостно и своевременно.

Актуализациите и промените трябва да спазват официален процес, който гарантира регистрирането на всички промени и осигуряването на възможност за отказ в случай на проблеми с новата версия.

Би следвало да се изисква официално одобрение преди програмите да преминат от нивото на тестова библиотека към производствена библиотека, а цялата документация за системите, операциите и програмите следва да бъде пълна, актуална и в съответствие със стандартите, политиките и процедурите.

» ПЛАНИРАНЕ НА НЕПРЕКЪСНАТОСТ НА ДЕЙНОСТТА И ПЛАН ЗА ВЪЗСТАНОВЯВАНЕ ПРИ БЕДСТВИЯ

Планирането на непрекъснатостта на дейността (ПНД) и свързаният план за възстановяване при бедствия (ПВБ) са насочени към постигане на целта за разполагаемост. Планирането за извънредни ситуации и възстановяване при бедствия, план за жизнеспособност, тестване и мониторинг, както и необходимостта от постоянно актуализиране на плановете са фактори от решаващо значение.

ПНД е цялостен подход за осигуряване на алтернативни възможности в подкрепа на критичните за дейността процеси в случай на аварии, бедствия или други подобни обстоятелства. Ударението пада върху оцеляване на цялата система, свързана с дейността, а не само на ИТ системата. Обаче цялостният план трябва да включва конкретни съображения относно изискванията на информационните системи и на телекомуникационната мрежа. Тази част от ПНД е също и ПВБ.

ПНД и свързаният ПВБ могат да бъдат разработени едновременно, така че всички аспекти да бъдат взети под внимание в синхрон. Като минимум, планът трябва да включва процедури и критерии за определяне кога дадена ситуация представлява бедствие, лицето, което отговаря за това и как официално да се обяви бедствено положение и да се задейства планът.

3. КОНТРОЛИ НА ПРИЛОЖЕНИЕТО

Контролите на приложението са автоматизирани контроли в приложенията на информационните системи, с чиято помощ се осигурява оторизиране, интегритет, точност и валидност на транзакциите. Те са вградени в програмирането на приложенията и са преобладаващи при входящите, обработващите и изходящи операции на приложенията. Целта им е да гарантират целостта, надеждността и точността на обработването на данните.

Сред примерите за контроли на приложението са проверките, които приложението прави на формата на въвежданите данни с цел предотвратяване въвеждането на невалидна информация, контроли на обработването, които предпазват потребителите от извършване на неразрешени транзакции и подробни доклади и контроли върху общия брой на транзакциите за гарантиране, че всички те са пълно и точно регистрирани.

Контролите на приложението могат да бъдат класифицирани по следния начин:

- входящи (на „входа”),
- на обработката, и
- изходящи (на „изхода”).

3.1. СТАНДАРТИ ОТНОСНО ДОКУМЕНТАЦИЯТА

Стандартите относно документацията гарантират, че се съхранява адекватна и актуална документация. Внимателното актуализиране на документацията също е важно.

Подходящата документация е важна за определяне на това какви са или какви трябва да бъдат контролите.

Добрата документация относно приложенията намалява също и риска потребителите да не спазват процедурите за контрол по начина, предвиден от ръководството. Прегледът на всеобхватната,

актуализирана документация помага на одитора да разбере как работи всяко приложение и може да е полезно за идентифициране на конкретни одитни рискове.

• Документация на приложенията: Помага на програмистите по поддръжката да разберат приложението, да отстранят проблемите и да направят подобрения. Документация се създава на всеки етап от процеса на разработването и може да има разнообразна форма, като схеми, графики, таблици или текст. Документацията може да включва подробности относно източника на данните, реквизити на данните, входни екрани, валидиране на данните, процедури за сигурност, описание на изчисленията, програмен дизайн, интерфейс с други приложения, контролни процедури, справяне с грешките, операционни инструкции, процедури за архивиране, резервни копия, съхраняване и възстановяване. Документацията на приложенията следва да се актуализира при модифициране на което и да е приложение.

• Потребителска документация: Включва описания както на автоматизирания, така и на ръчния работен поток в помощ на първоначалното обучение, а и за текущи справки.

Във всички случаи, потребителската документация подлежи на актуализация при модифициране на приложенията.

Документацията следва да включва:

- общ преглед на приложението;
- спецификация на потребителските изисквания;
- описания и списъци на програмите;
- описания „на входа”/”на изхода”;
- описания на съдържанието на файловете;
- ръководства за потребителя;
- настолни инструкции;
- описания на контролите за сигурност на приложенията;
- скорошни резюмета на оценките на сигурността;
- скорошни решения относно сигурността и препоръчани действия, и
- състояние на препоръчаните действия.

3.2. КОНТРОЛИ НА „ВХОДА”

Контролите на входящо ниво са изключително важни за намаляване на риска от грешка или измама при компютризираните приложения.

Контролите на входа са от решаващо значение за интегритета на данните.

Контролите на входящо ниво помагат за гарантиране на оторизацията, точността, целостта и навременността на данните, въведени в приложението. Оторизацията се гарантира посредством вторично одобрение на транзакциите, които надвишават определен праг. Точността се гарантира чрез редакционни проверки, които валидират данните преди приемане на дадена транзакция за обработка. Целостта се гарантира чрез процедури за справяне с грешките, които се отнасят до регистриране, докладване и отстраняване на грешки. Навременността се гарантира чрез мониторинг на потока от транзакции, регистрирането и докладването на изключения.

Контролите на входящо ниво могат да бъдат при:

- екраните на входящи данни;
- рутинните процедури за подготовка на данни;
- оторизацията на входящи данни;
- съхранението на входящи документи;
- валидиране на входящи данни;
- процедурите относно грешки при въвеждане на данни, и
- подкрепящите механизми при въвеждането на данни.

Контролите, описани по-горе биха могли да бъдат заобиколени в случай, че подобно заобикаляне е възможно, посредством въвеждане или промяна на данните извън самото приложение. Необходимо е да съществуват автоматизирани проверки на интегритета на приложението, които разкриват и докладват всяка промяна на данните от външен източник. Например, трябва да има заложена проверка, която да разкрива и докладва всяко неразрешено изменение, направено в основната база данни на транзакциите.

» ЕКРАНИ ЗА ВХОДЯЩИ ДАННИ

Стандартизираните екрани за входящи данни могат да осигурят последователност при въвеждането на данните.

ИСУПД може да включва следните функции:

- входни екрани в стандартизиран формат и оформление;
- полета за въвеждане на данни, които налагат ограничения върху това, което е разрешено да въвеждат потребителите;
- определени задължителни за попълване полета; и
- функция „помощ” (напр. F1), която подпомага потребителите при

попълване на полетата за въвеждане на данни.

» РУТИННИ ПРОЦЕДУРИ ЗА ПОДГОТОВКА НА ДАННИ

Целта на рутинните процедури за подготовка на данни е да се избегнат неуспехи по време на процедурите по въвеждане на данни.

ИСУПД може да включва вградени среди за процедури за споделяне на данни с цел прехвърляне на данните към други приложения.

» ОТОРИЗАЦИЯ ЗА ВЪВЕЖДАНЕ НА ДАННИ

Разрешението за въвеждане на данни цели да гарантира, че всички въведени данни са записани и оторизирани от подходящото лице.

ИСУПД може да включва следните функции:

- изискване на парола за достъп;

- запис на файла за достъп, когато има ръчно въвеждане на данни, и

- изискване за двойно одобрение на някои чувствителни операции (напр. задействане на договори, промени в нивата на лихвени проценти, изменения в стойностите по договори).

» ЗАПАЗВАНЕ НА ВХОДЯЩИТЕ ДОКУМЕНТИ

Тази област от контролите на входящи данни се отнася до поддръжката и контрола върху оригиналните документи в подкрепа на записите на данни за дълг. В случай, че има автоматично прехвърляне на файлове между приложенията, ИСУПД трябва да съхранява данните получени от други приложения за период от време, който е предварително определен от СУД.

» ВАЛИДИРАНЕ НА ВХОДЯЩИ ДАННИ

Контролите за валидиране на данни се разработват с цел да се гарантира, че входящите данни са валидни и точни.

ИСУПД може да включва следните функции:

- автоматизирани контролни листове проверяват липсата на стойности (напр. при изтегляне на историческа серия от показатели, ИСУПД проверява дали липсва дневна, месечна или годишна стойност);

- Всички екрани за входящи данни ясно показват кои са задължителните полета, а приложението разрешава потвърждаване на операцията единствено, когато е въведена цялата задължителна

информация;

- Всяка таблица с база данни трябва да съдържа конкретно правило относно полетата, където не е разрешено дублиране на данни;

- Ако приложението счете, че са въведени дублирани данни, то няма да приеме въвеждането, докато не бъде отстранено дублирането;

- Приложението не позволява изменението на определени данни след като веднъж са въведени (напр. обменен курс на датата на операцията). По отношение на други данни, приложението би могло да разреши изменения при положение, че са изпълнени определени условия (напр. когато даден договор е със статут „заключен" или „сключен", данните не могат да се променят).

- При попълване някои полета изискват да бъдат попълнени и други полета (напр., ако потребител въведе таксата за ангажимент по договор, този потребител трябва също да попълни и данъка за ангажимент).

- Полетата за дата са изключително важни за общия контрол върху договорите за дълг. Те са особено полезни при изчисляване на вноските, за да се избегне забавяне на плащания, налагане на глоби и т.н. В този смисъл, приложението трябва да има определени правила относно вмъкването на датата.

- С изключение на симулираните операции, системното приложение не позволява регистриране на данни за бъдеща дата, напр. разплащане, обратно разплащане, отмяна на договор или добавяне на договор.

» ГРЕШКИ ПРИ ВЪВЕЖДАНЕ НА ДАННИ

Одитната следа или одитния регистър е от значение за сигурността и представлява хронологичен запис, набор от записи, или дестинация или източник на записи, които предоставят документални доказателства за последователността от дейности, които във всеки момент са повлияли върху конкретна операция, процедура или събитие. Одитната следа или файловете от регистъра/архива следва да бъдат достъпни само за подходящия персонал.

ИСУПД може да включва следните функции:

- СУД следва да определя отговорността по отношение на необработени/"чакащи" файлове;

- Програми за грешни действия при регистрацията, докладване на грешки и записване на корекции на грешки следва да бъдат вградени в приложението;

- При процес на автоматизирано сваляне на данни, когато приложението идентифицира пропуски в сериите, автоматично електронно съобщение се изпраща до подходящите потребители с цел

последващи действия; и

- Приложението следва да изпраща на подходящия персонал периодични доклади относно неотстранени грешки, включително и колко време грешките са останали неотстранени и техният приоритет.

» ПОДКРЕПЯЩИ МЕХАНИЗМИ ПРИ ВЪВЕЖДАНЕТО НА ДАННИ

Тези контроли са свързани с подкрепящите процедури в СУД, които помагат на потребителите да въвеждат данни в компютърното приложение, повторно инициализиране на приложения и мониторинг на потребителските дейности за избягване на евентуални отклонения от установените правила.

Тези механизми често са включени в общите контроли.

3.3. КОНТРОЛИ НА ОБРАБОТКАТА

Контролите на обработката гарантират точността, пълнотата и навременността на данните по време на партидна или онлайн обработка. Тези контроли помагат да се гарантира точната обработка на данните чрез приложението, както и че няма добавяне или промяна на данни по време на обработката.

» ПЪЛНОТА

Пълнотата може да бъде осигурена при партидната обработка чрез балансиране на транзакциите, получени в системата с транзакциите, изпратени от спомагателна система.

Балансирането следва да се осъществи между приложения, които споделят общи данни, чрез създаване на съгласувателен доклад, който описва данните от двете приложения и докладва наличието на различия за дадена потребителска група.

Балансовите общи стойности трябва да включват брой на транзакциите и общи стойности за всички количествени полета, както и обобщени стойности за полетата с подробности към полетата с общи стойности.

При файлове в които няма смислени общи стойности, може да се създадат хеш стойности, които да събират всички цифри в дадена колона, за да се потвърди, че същата стойност е приета от следващия процес. Например, обща стойност на номерата на споразуменията за дълг не е смислена стойност, но тя може да се използва, за да се провери дали всички коректни номера на споразумения за дълг са включени в обработката.

ИСУПД може да включва следните функции:

- В интерфейса с други системи между приложенията, в случай на грешка в обработката на файлове се генерира файл за грешка, който се записва в системното приложение. Потребителите трябва да развият по-задълбочен оперативно-съвместим подход спрямо техническите профили и обучението в съответната организация.

- Приложението съдържа планирана партидна обработка на множество задачи, напр. актуализация на запасите, финансово планиране, показатели/индекси и бъдещи плащания. Потребителите трябва да оценяват „меките" изходящи данни от системата в реално време, фокусирайки се върху базираните на партиди регистри, както и „твърдите" способности в реално време за измерване на обработката на актуална информация.

- В случай на грешка при обработката на партидите, приложението изпраща съобщение да потребителя с информация за грешката. Потребителят може да провери консолидиращите възможности вътре в системата за изпълнение на политиките относно коригирането на грешки и за конфигуриране на контролните процедури.

- След приключване на операция, приложението показва съобщение, което потвърждава, че обработката е успешна и представя резюме на въведените данни.

- След модифициране на вече регистрирани данни, приложението показва съобщение, че модификацията е успешна и представя резюме на модифицираните данни.

- След изтриване на вече регистрирани данни, приложението показва съобщение, че изтриването е успешно и представя резюме на изтритите данни.

- В случай, че изтриването на запис засяга релационния интегритет на базата данни, приложението не разрешава изтриването и показва съобщение, че записът не може да бъде заличен. Например данните на банка-кредитор не могат да бъдат заличени от таблицата на кредиторите, ако този кредитор има договори в процес на изпълнение в приложението.

- Приложението извършва някои проверки на данните на фронт офиса и на бек офиса. Например, изисква от бекофиса да валидира входящите данни от аукциони. Потребителите могат да проверят комуникациите за взаимовръзки на архитектурата на данните между компонентите и системите, за да верифицират потоците данни съгласно диаграмата за оперативна съвместимост.

3.4. КОНТРОЛИ НА „ИЗХОДА”

Контролите на „изхода” гарантират интегритета на резултатите и коректното и своевременно разпределение на генерираните резултати. Слабости в обработката могат понякога да бъдат компенсирани със засилени контроли „на изхода”. Дори и добре контролираното приложение „на входа” и при обработката има вероятност да се обезсмисли напълно, ако липсва контрол „на изхода”.

Пълнотата и интегритета на докладите „на изхода” зависят от ограничаване на възможността за промяна на резултатите и включване на проверки за пълнота, като напр. номера на страници и проверки на сборовете.

Файловете с резултатите/ „на изхода” трябва да бъдат защитени, за да се намали риска от неразрешени промени. Възможните мотиви за внасяне на изменения в компютърните резултати включват прикриване на неоторизирана обработка или манипулиране на нежелани финансови резултати.

Изходните резултати от едно ИТ приложение биха могли да формират входящи данни за друго приложение. Когато това е така, авторът трябва да види контролите, за да гарантира, че изходните резултати са правилно прехвърлени от един етап на обработка към следващ етап.

В ИСУПД контролите „на изхода” могат също да бъдат програмирани да идентифицират критична информация, която изисква приоритетни действия от страна на управлението на публичния дълг. Например във връзка с договори, които изтичат през текущия месец, приложението би могло да показва ежедневни напомняния на първия екран на системата за договорите, чиито дати на плащане изтичат през следващите 5 дена.

Приложението може също да позволява на някои профили на потребители да генерират доклади в приоритетен режим, като по този начин дава възможност на приложението да подрежда по приоритет докладите, които се генерират.

ИСУПД може да включва следните функции:

- приложението предоставя автоматизирано сравнение на сумите от първоначалните данни със сумите от обработените данни;

- приложението трябва да информира потребителите за статуса на искането за генериране на доклад, например „не е стартирано”, „в процес на извършване” и „приключено”; и

- в края на процеса на генериране на доклад, приложението изпраща съобщение на потребителя, който е подал искането, като го информира, че задачата е изпълнена.

3.5. ТЕСТВАНЕ НА КОНТРОЛИТЕ НА ПРИЛОЖЕНИЯТА

След идентифицирането на контролите, следващата стъпка е одит за проверка на ефективността им.

Това може да се постигне чрез:

- подаване на набор от тестови данни, които, когато приложението работи

правилно, ще произведат познати резултати;

- разработване на независими програми за повторно изпълнение на логиката на приложението; и

- оценяване на резултатите от приложението.

Горните процедури тестват интегритета на програмата вградена в ИСУПД, а не интегритета на данните.

Ако приложението има тестваща среда, това може да се използва за тестване на контролите, стига тестващата среда да е потвърдено копие на производствената среда.

За тестване на правилата на изчисляване, като тези, които се отнасят до актуализиране на запасите или обслужването на дълга, одиторът може да има нужда от компютърни техники за одит (CAAT), които включват множество видове инструменти и техники, като напр. генерализиран одиторски софтуер, помощен софтуер, тестови данни, приложен софтуер за проследяване и картографиране и експертни одиторски приложения. Може да бъдат включени и инструменти, които правят анализ за точност на логиката и изчисленията в електронните таблици. Инструменти могат да се ползват и за анализ на приложенията на базите данни и за изготвяне на логически схеми. Генерализираният одиторски софтуер може да се използва за анализ на данни, произведени от повечето приложения.

Одиторът следва да оцени необходимостта от ползване на CAAT. Използването им трябва да се основава на сложността на приложението за управление на публичен дълг.

Настоящият документ съдържа предложение за тестваща матрица (вж. Приложение III), която евентуално да се ползва от одиторския екип за справка при тестване на контролите на приложенията. Тази матрица идентифицира някои от изискванията и функциите, които системите в областта на публичния дълг следва да предоставят, заявки, които да може да изпълняват, както и минималните изисквания относно капацитета на подобни системи.

Важно е да отбележим, че тъй като дългът на всяка страна има различен състав и характеристики, системите за управление на дълга също имат

различни характеристики. В този смисъл, одитният екип отговаря за идентифицирането, коригирането, при необходимост, и използването на елементите, приложими към дълговата система на своята държава.

3.6. ДОКЛАДВАНЕ НА ОДИТНИТЕ РЕЗУЛТАТИ

В допълнение към спазването на Декларацията от Лима относно указанията за одитните насоки, когато е подходящо, докладването на одити на ИСУПД трябва да отговаря на изискванията на МСВОИ 5440, Указания за извършване на одит на публичен дълг – използване на тестове по същество при финансови одити, раздел 2.6 Докладване на одитни резултати.

Както беше отбелязано, одитът на ИСУПД е одит на изпълнението, затова е важно докладът да спазва стандартите за докладване на одити на изпълнението, както е указано в МСВОИ 3000 , Стандарт за одит на изпълнението и МСВОИ 300, Основни принципи на одита на изпъл

ПРИЛОЖЕНИЕ I:
ТАБЛИЦА ЗА ПЛАНИРАНЕТО

Необходима информация, документи и доклади
- Опис на информационните системи, използвани в СУД и свързаната документация за системите; - Опис както на компютърните, така и на мрежовите операционни системи използвани от СУД; - Актуална схема на последователността на процесите в СУД; - Предишни одитни доклади от одити на СУД; - Предишни одитни доклади, свързани с ИТ системите на публичния дълг; - Закони и нормативни разпоредби, свързани с рамката на СУД и управлението на публичния дълг; - Списък на ръководителите на СУД и на ИТ, на управлението за непрекъснатост на дейността, на човешките ресурси, управлението на риска, вътрешния одит и други, техните задължения, адреси, и-мейл адреси и телефони; - Документи, които показват функционирането на СУД, нейните системи, или писмените политики и процедурни ръководства на СУД или министерство на финансите, както следва: • Управление на персонала; • Управление на промяната; • Физически достъп; • Изисквания на ИТ средата/местоположението; • Логически достъп; • Планиране за непрекъснатост на дейността (ПНД); • План за възстановяване при бедствия (ПВБ); • Резервен план; • Услуги от трети страни (ИТ услуги); • Доклади от предварителна оценка на риска; • Скорошно резюме на оценките на сигурността; • Скорошни решения по отношение на риска и препоръчани действия; • Статус на препоръчаните действия; • Одобрение от страна на висшето ръководството за

експлоатация на системата.

- Доклади на външни организации, натоварени с осигуряване на поддръжката на системата;
- Други документи, свързани със СУД, нейните системи, или и двете (напр. слайдове, текст, цели и годишни доклади, свързани с управлението на дълга);
- Брой на служителите на СУД, които са потребители на системата и техните профили за достъп;
- Брой на ИТ служителите и длъжностните им характеристики (определение на ролите им), както за персонала на СУД, така и за ИТ персонала;
- Списък на служителите с достъп до помещението със сървъра;
- Описание на профила за достъп в ИСУПД;
- Официално описание на начина и периода на актуализация на операционната система, защитните стени и антивирусния софтуер;
- Роля на физическите препятствия и автоматизираните инструменти за предотвратяване на неразрешен достъп до мейнфрейми, работни станции, сървъри и други съоръжения на СУД;
- Местоположение на всяко помещение вътре и извън СУД;
- Списък на персонала, работните станции и сървъри;
- Разпределение на бюджета за последните 5 години;
- Опис на предварителното обучение, както за използване на ИСУПД (персонал на СУД), така и за актуализация на ИТ (ИТ персонал);
- Установени правила, практики и вградени описания за предотвратяване на вреди, причинени от нестабилност в електрозахранването, пожар, прах, вода, екстремни температури, влажност или статично електричество;
- Спецификации относно функционирането при непрекъсваемо електрозахранване (ако има);
- Регистър/архив на инцидентите при поискване от СУД относно грешки на ИСУПД;
- Доклади от регистъра/архива на инциденти, свързани сигурността;
- Опис на промените в ИСУПД от последните 12 месеца;
- Регистри и доклади от предходни тестове на ПНД и ПВБ и реални събития;

- Документация за приложението и потребителя;
- Условия за ползване на всяко приложение;
- Процедурно ръководство за справяне с грешки в обработката;
- Образец от данните за повторно извършване на операциите с цел тестване на контролите на приложението и изчисленията.

Процедури

- Запознаване с документацията на системата (ръководства и условия за ползване), за да бъдат разбрани основните процеси във връзка с дълга, които извършва информационната система; ако документацията за процесите в СУД е недостатъчна, одитният екип следва да проучи и определи процесите;
- Потвърждаване на наличието на нормативни правила по отношение на използването, поддръжката и бизнес управлението на ИСУПД;
- Идентифицирани в предишни одити констатации, свързани със слабите точки в оперативния поток на публичния дълг, на системите за управление на публичния дълг, или и двете;
- Идентифициране на общите контроли на приложенията на базата на документацията на системата
- Идентифициране на главните общи контроли на базата на документацията на системата: въвеждане на данни, обработка и контрол „на изхода";
- Извършване на оценка на риска при тези главни общи контроли и контроли на приложението, за да се оцени кои рискове влияят върху тези системи и колко сериозно е това влияние върху системата за управление на дълга;
- Установяване кои системи влияят върху критичните функции и данни, като въвеждане, обработка и краен резултат, списъци с кредитори, изчисления във връзка с публичния дълг, докладване и взимане на решения;
- Идентифициране на вътрешните контроли, които се прилагат с цел смекчаване или намаляване на установените рискове;
- Класиране на системите и процесите съобразно оценката на риска и определяне на обхвата на одита;
- Преценка на ресурсите и графика;

- Уговаряне на интервюта с ръководителя на ИТ звеното, директорите и техническия орган, които отговарят за работата по разработване/ поддръжка/експлоатация на системата;
- Разработване на матрица за одита на общите контроли и контролите на приложенията и определяне какви тестове да бъдат проведени (вж. матрицата, предложена в Приложение III);

ВОИ следва да отговорят на следните въпроси

- Кои са информационните системи за управление на публичния дълг и каква е ролята на всяка от системите в управлението на дълга?
- Единствено СУД ли е разработил ИСУПД или я е получил от трета страна? Във втория случай, правени ли са някакви настройки за персонализиране с цел удовлетворяване на специфични за СУД потребности?
- С кого в СУД следва да се проведат интервюта по въпросите, свързани с общите ИТ контроли?
- С кого следва да се проведат интервюта относно изясняване на контролите на приложенията на ИСУПД?
- Кои са основните потребители на ИСУПД?
- Кои са общите контроли и контролите на приложенията на ИСУПД?
- В състояние ли са вътрешните контроли да намалят ИТ рисковете, които биха могли да повлияят върху управлението на публичния дълг?
- Кои са най-големите рискове по отношение на въвеждането на данните, обработката и крайните резултати от ИСУПД?
- Какви тестове на общите контроли и контролите на приложенията следва да бъдат проведени?

ПРИЛОЖЕНИЕ II:МАТРИЦА ЗА ТЕСТВАНЕ НА ОБЩИТЕ КОНТРОЛИ

ОБЩИ КОНТРОЛИ		
Целите на общите контроли е да опазват данните, да защитават програмите на приложенията и да гарантират непрекъснатост на компютърните операции в случай на неочаквано прекъсване.		
ИЗИСКВАНЕ/ ФУНКЦИОНАЛНОСТ	**ОБЩ КОНТРОЛ**	**ПРЕДЛОЖЕНИЯ ЗА ТЕСТВАЩИ ПРОЦЕДУРИ**
Общи въпроси	Действията на ИТ сектора трябва да са съобразени с мисията на СУД; Необходимо е да има мониторинг върху изпълнението на ИСУПД от гледна точка на целите на СУД; Периодично следва да се провежда вътрешен одит на операциите, извършвани от СУД/ИСУПД;	Извършване на проверка на извадка от управленски решения или документи по отношение на ИТ дейностите, за да се установи, че те са ясни, добре обосновани и съобразени с мисията на СУД; Оценяване на мерките за ефективност на ИСУПД спрямо очакваните показатели и гарантиране, че висшето ръководство признава мерките; Оценка на доклади от предишни вътрешни одити на общите ИТ контроли за установяване на сериозни недостатъци; Оценка както на относителния брой, така и на възможностите на ИТ работните станции и другите ИТ устройства и потвърждаване, че

		персоналът притежава необходимите умения Оценка на относителния размер на бюджета и сравняване с бюджета от предходни периоди и с ИТ секторите на други правителствени организации;

Организационни контроли	Ръководството на СУД или на Министерството на финансите следва да е ангажирано с разработването и поддържането на добра обща ИТ среда; Персоналът на СУД и ИТ персоналът следва да участват в периодично и адекватно обучение, което включва и повишаване на информираността относно сигурността; Трябва да има програма за обучение; Трябва да съществуват писмени политики и стандартни процедури относно: • Информационната сигурност; • Човешките ресурси; • ИТ услуги от трети страни; • Управление на промяната; • Физически и логически достъп; • Планиране на непрекъснатостта на дейността и плановете за възстановяване при бедствия; • Политиките и стандартните процедури следва да се актуализират периодично; • Политиките следва да бъдат адекватно	Провеждане на интервюта с висшето ръководство на СУД относно интересът им към ИТ, с цел оценка на ангажимента им за разработване и поддържане на добра обща ИТ среда; Преглед на доказателствата за провеждане на обучения; Провеждане на интервюта с ИТ персонала относно: • Честота на обучение; • Потребност от знания/ обучение; • Знания за политиките; Оценка на адекватността на писмените политики и стандартните процедури, отнасящи се до ИТ услугите; Наблюдения дали ИТ персоналът работи в съответствие със стандартните процедури (залегнали в писмено ръководство);

	разпространени от висшето ръководство; • Служителите на СУД трябва да познават тези политики; • Следва да има документирани процедури за всички дейности, които се отнасят до управление на дълга; • Организацията следва да прилага подходящо разделение на задълженията, за да се гарантира, че никой потребител не притежава повече правомощия от необходимото за конкретната му работа.	
Физически контроли	Физическият достъп до мейнфрейма и сървърите трябва да бъде ограничен (напр.използване на врати, ключалки и т.н.); Трябва да има видеонаблюдение; Прозорците на помещението, където са разположени мейнфрейма и сървърите трябва да бъдат защитени срещу насилствено влизане; Всеки, който влиза в помещението на	Проверка на наличието и ефективното функциониране на физически препятствия, които предпазват от неразрешен достъп до мейнфрейма, сървърите и работните станции на СУД; Проверка дали административните процедури спрямо персонала, целящи предотвратяване на неразрешен достъп и намеса в ИТ услугите, работят съгласно

	сървъра трябва да има разрешение за това;	официално установени правила; С цел идентифициране на евентуални слабости в автоматизираните контроли, извършване на наблюдения върху работата на електронните устройства, като напр. електронни брави и заключващи системи, камери и други способи за ограничаване на физическия достъп до сървърите и другата критична инфраструктура; Когато има електронни заключващи системи, проверка относно споделянето на пароли между служителите.
Логически контроли	Ако ИТ услугите, отнасящи се до управлението на публичния дълг са възложени на външни изпълнители, договорът следва да определя адекватни контроли, гарантиращи, че трети страни няма да имат достъп до секретна информация, важни данни и стратегии относно дълга;	Оценка дали профилите за достъп се основават на ролите на служителите; Проверка дали някой бивш служител или лице, което не работи за СУД не разполага с активен профил за достъп; Проверка за наличност на защитни стени и

	Не трябва да има нито един бивш служител, лице, което не работи за СУД, или пък „виртуален” потребител с активен профил за достъп. Правата за достъп следва периодично да се преразглеждат; Актуализираните антивирусни програми, защитни стени и софтуер за разкриване на намеса и зловредни действия следва да работят; Трябва да се прави систематична актуализация на оперативната система на работните станции и сървъри; Организацията следва да е определила процедури за гарантиране, отнемане или изменение на контрола на достъпа при промяна в условията (новонаети или съкратени служители, изменения в задълженията и т.н) Организацията следва да оповести своята политика или указания относно паролите и другите контроли в областта на сигурността (ключ карти и	актуализирани антивирусни програми и софтуер за разкриване на намеса и зловредни действия; Проверка относно систематичното актуализиране на операционната система на работните станции и сървърите; Оценка относно правилното прилагане на политиката спрямо паролите; Проверка дали процедурите са дефинирани и документирани;

	др.) на всички потребители на ИСУПД.	
Контроли на средата	През помещението на сървъра следва да минават тръби (за вода, отопление, електричество и т.н); Трябва да има датчици за вода, топлина и влажност; В помещението на сървъра трябва да има система срещу наводняване; Трябва да има пожароизвестителни датчици / датчици за пушек. Подът трябва да е повдигнат или оборудването да е поставено на 15-20 см от пода или стелажите;	Инспекция и оценка на условията на средата в помещението на сървъра с базата данни; Проверка за наличие и ефективна поддръжка на устройствата за предпазване от пожари, наводнения и влажност; Проверка на наличието и ефективното функциониране на алтернативното захранване, за да не бъдат прекъснати ИТ услугите;
Контроли на промени в програмите	Ръководството на ИТ трябва да поддържа одитен регистър на оперативни проблеми, инциденти и грешки; Регистърът следва да проследява всеки инцидент – от причината до решението; На *хелпдеска* не бива да остават нерешени въпроси относно инструкциите за ИСУПД; Трябва да има процес за ескалиране на проблеми в критични ситуации и	Оценяване на времето, отделено за решаване на искания от страна на СУД във връзка с инструкциите за употреба или откази във функционирането на ИСУПД; Идентифициране на по-честите откази в работата на ИСУПД и вероятните причини; Сравняване на предварителните промени със стандартните

	подходящо ниво на реагиране съобразно приоритета на събитието; Трябва да има доклад за събитие, свързано със сигурността, който е предоставен на ръководството на СУД; Предварителните промени трябва да спазват стандартни процедури; В случай, че се използва нестандартна система за управление на дълга, организацията трябва да е документирала своята процедура за контрол на промяната и да е описала кой е оторизиран да внася промени в системата; Организацията следва да проследява и наблюдава всички промени в системата (одитна следа).	процедури.
ПНД и ПВБ	СУД следва да разполага с ПНД и ПВБ; Персоналът, отговорен за непрекъснатостта на операциите следва да е наясно с ролята и задълженията си; Слабостите при предишни тестове на ПНД и ПВБ или при реални събития и дейностите, предприети от СУД за	Оценяване на последователността и пълнотата на ПНД и ПВБ, както и дали са актуализирани; Оценяване на доклади от предишни тестове на ПНД, ПВБ и резервния план; Проверка дали ПНД и ПВБ са сведени до знанието на целия

	справяне с тях следва да бъдат докладвани; Кредитната документация трябва да се съхранява добре и да бъде защитена от кражба, пожар, наводнение или други инциденти, които биха могли да я увредят или унищожат.	персонал; Проверка дали резервните копия извън обекта са в добро състояние и дали могат да бъдат използвани за рестартиране на системата в случай на повреда.

ПРИЛОЖЕНИЕ III:МАТРИЦА ЗА ТЕСТВАНЕ НА КОНТРОЛИ НА ПРИЛОЖЕНИЕТО

СТАНДАРТИ ЗА ДОКУМЕНТАЦИЯТА		
Целите на добрите стандарти за документация са да гарантират, че контролите ще работят постоянно и ще намаляват риска от грешка.		
ИЗИСКВАНЕ/ ФУНКЦИОНАЛНОСТ	**ОБЩ КОНТРОЛ**	**ПРЕДЛОЖЕНИЯ ЗА ТЕСТВАЩИ ПРОЦЕДУРИ**
Контроли на документацията	Документацията на приложението следва да бъде достатъчно всеобхватна (като включва всички функции на приложението и свързаните с тях действия)	Проверка на документацията
	Документацията следва да бъде актуализирана, за да отразява всяко изменение в приложението	Проверка на документацията
	Контролите на приложението, които са включени в документацията следва да са внедрени и да работят ефективно	Проверка на извадка от контролите на приложението за установяване дали са внедрени съгласно документацията и дали работят ефективно
Архивиране на документация (backup)	Следва да се съхранява архивирано резервно копие на документацията	Проверка на архивираното резервно копие на документацията
КОНТРОЛИ НА „ВХОДА”		
Целта на контролите на „входа” е да се гарантира оторизацията, точността, пълнотата и навременността на данните, въведени в приложението.		

ИЗИСКВАНЕ/ ФУНКЦИОНАЛНОСТ	КОНТРОЛ НА ПРИЛОЖЕНИЕТО	ПРЕДЛОЖЕНИЯ ЗА ТЕСТВАЩИ ПРОЦЕДУРИ
Задължителни полета за въвеждане на данни	Приложението не позволява операцията да бъде потвърдена, ако някое от задължителните полета не е попълнено	Потвърждаване на операция при пропускане на задължителни данни и проверка дали транзакцията ще бъде обработена; Прилагане на теста към следните процеси: регистър на договори, задействане на договори; регистър на емитиране на ценни книжа и т.н.;
Коректно и подходящо въвеждане на данни	Приложението не приема въвеждането на некоректни или неподходящи данни	Проверка на формата на данните в базата данни; Преглед на спецификациите за въвеждане на данни и проверка на някои от тях в приложението; Опит за въвеждане на некоректни или неподходящи данни и проверка дали данните не биват приети и дали се генерира съобщение за грешка; Прилагане на тези тестове спрямо следните процеси: регистър на договори,

		задействане на договори; регистър на емитиране на ценни книжа, актуализиране на индекси, обратно изкупуване на ценни книжа и т.н.;
	Приложението не позволява дублиране на данни	Опит за регистриране на договор или ценна книга под съществуващи имена и проверка дали данните биват приети и дали системата генерира съобщение за дублиране
	Във връзка с лихвените проценти по договорите, не бива да съществуват припокриващи се или непокрити периоди по отношение на приложимостта на лихвените проценти	Проверка на базата данни за периоди с припокриващи се или непокрити лихвени проценти
	Когато става дума за договори за дарение, приложението следва да позволи вписването на плащанията, тъй като в този случай няма амортизационни и лихвени операции	Опит за въвеждане на разплащане от договор за дарение и проверка дали приложението не изисква амортизационни и лихвени операции
	На входния екран за разплащания, когато потребител търси договори, за да впише разплащане, приложението следва да показва единствено договори, чийто статус е	Опит за въвеждане на плащане и проверка какъв етап на договора показва приложението

	„активен” на етап на разплащане, или на разплащане и амортизация	
	Ако лихвеният процент е плаващ, приложението трябва да изиска ключването на индекса	Проверка дали приложението ще изиска индекс при избор на плаващ лихвен процент
	Приложението не трябва да позволява въвеждането на десетични номера за емитиран брой ценни книжа	Опит да се въведе десетичен номер за емитиран брой ценни книжа и проверка дали приложението ще приеме въвеждането
	Приложението трябва да позволи създаването на ценна книга преди емитирането й	Симулиране на създаване на ценна книга без реално емитиране
Пълнота на информацията	Цялата необходима информация относно дълга трябва да бъде въведена в приложението	Проверка дали цялата важна за дълга информация е въведена в приложението, напр. кредитни операции, гаранции, кредити, лихвени проценти и обменни курсове
Съответствие между датите	Началната дата за изчисляване на ставката за ангажимент следва да предхожда датата на приключване на проекта	Опит да се въведе начална дата за изчисляване на ставката за ангажимент, която е след датата на приключване на проекта,

		както и проверка дали датата не бива приета и дали се генерира съобщение за грешка
	Ефективната дата следва да бъде по-ранна от датата на крайния срок за плащане	Опит да се въведе ефективна дата, която е по-късна от крайния срок на плащането и проверка дали датата е приета и ако не дали се генерира съобщение за грешка
	Датата на краен срок за разплащането следва да е по- ранна от датата на приключване на проекта	Опит да се въведе дата на краен срок за разплащане, която е по- късна от датата на приключване на проекта и проверка дали датата е приета и дали се генерира съобщение за грешка
	За да се получи доклад относно падежа, крайната дата на падежа на ценна книга трябва да е по-ранна от началната дата	Опит да се въведе начална дата, която е по-късна от крайна дата на падеж и проверка дали датата е приета и дали се генерира съобщение за грешка
	Приложението не приема бъдещи дати на операции	Опит да се извършат някои операции, като се въведе бъдеща дата и проверка дали датата е приета и дали се генерира съобщение за грешка;

		Прилагане на този тест спрямо следните процеси: регистър на договори, задействане на договори; регистър на емитиране на ценни книжа, актуализиране на индекси, обратно изкупуване на ценни книжа, разплащане, записване, добавяне на договор и т.н.;
	Датата на емитиране на ценна книга следва да е по-ранна от датата на падежа	Опит да се въведе дата на издаване, която е по-късна от датата на падежа и проверка дали датата е приета и дали се генерира съобщение за грешка
	При регистрирането на плащания по погасителен план, в случаите, когато сумата или датата са различни от тези в приложението, приложението следва да покаже съобщение, което информира потребителя относно тази ситуация преди потвърждение, че операцията може да бъде приключена	Регистриране на плащане на стойност или на дата, която е различна от датата в приложението и проверка дали приложението показва съобщение
	Ако датата на ликвидация е различна от датата на падеж, приложението трябва да изисква да бъдат попълнени	Въвеждане на различни дати за матуритет и ликвидация и

	полетата „обосновка” или „заверка от кредитор”	проверка дали приложението изисква обосновка или заверка
	Планираните разплащания не могат да имат припокриващи се периоди; напр. началната дата на второто разплащане не може да предшества крайната дата на първото разплащане	Опит да се въведе дата на второ разплащане, която е по-ранна от крайната дата на първото и проверка дали датата е приета и дали се генерира съобщение за грешка
Сигурност на въвеждането на данните и на операциите	Приложението не трябва да разрешава на неоторизирани лица да въвеждат определени данни, нито да извършват определени операции	Проверка дали съществуват определени символи или други изисквания спрямо конкретни потребителски профили; Опит да се въведат данни и да се извършат операции без наличие на подходящия профил и проверка дали това е възможно; Прилагане на този тест спрямо следните процеси: регистър на договори, задействане на договори; регистър на емитиране на ценни книжа, промяна в индекс, обратно

		изкупуване на ценни книжа, записване на плащане и т.н.
	Приложението трябва да записва архив на достъпа при ръчно вкарване на данни	Проверка на регистрите с ограничен достъп и гарантиране, че регистрите не могат да бъдат видени или модифицирани от лица, които не са одобрени
	Приложението не трябва да позволява промяна в стойности на активен договор	Опит за промяна в стойността на активен договор и проверка дали това е позволено
	Приложението следва да предотвратява промяна на данни и заличаване на договори, чийто статут гласи „канцелиран” или „приключен”	Опит за промяна или изтриване на някакви данни в извадка от договори със статут „канцелиран”или „приключен” и проверка дали това е разрешено
	Приложението не трябва да позволява изтриването на активен договор, освен ако договорът не е в процес на договаряне	Опит за изтриване на активен договор, който не е в процес на договаряне и проверка дали това е разрешено
	Приложението не трябва да позволява неправилното изключване на емитирана ценна книга, освен ако няма	Опит за изтриване на емитирана ценна книга, която не е свързана с

	операция свързана с тази книга	операция и проверка дали това е разрешено
	Приложението трябва да изисква двойна оторизация за извършване на критични операции	Проверка дали критичните операции изискват двойна оторизация, за да бъдат приключени; Прилагане на този тест спрямо следните процеси: регистър на договори, емитиране на ценни книжа; плащания по погасителен план, обратно изкупуване на ценни книжа, промени в стойността на договор, изплащане на талони, обратно плащане, промени в лихвените проценти и т.н.
	Приложението трябва да приема въвеждане на данни единствено от признати източници; въведеният заем трябва да съответства на договора и приетите стандарти	Проверка за въвеждане на основни данни два пъти и установяване дали излиза съобщение за грешка, когато в тях има разлика
	Приложението следва да позволява намаляване на договорна стойност, стига тя да не е по-голяма от стойността на „салдото за разплащане”	Опит да се намали договорна стойност като се надскочи стойността на салдото за изплащане и проверка дали данните биват

		приети и дали се генерира съобщение за грешка
	Приложението трябва да записва всички транзакции само по веднъж	Извършване на идентични транзакции (напр. плащане на погасителни вноски) и проверка дали транзакциите не се обработват и дали не се дублират в базата данни
	При регистриране на плащане, когато разрешението на потребителя е анулирано, приложението трябва да докладва анулирането едва, когато потребителят опита да въведе плащането, като по този начин регистрира както неуспешния опит, така и данните, които е възнамерявал да въведе потребителят	Опит да се регистрира плащане с анулирано разрешение и проверка дали данните не биват приети и дали опитът бива регистриран
	В случаи на автоматично прехвърляне на файлове между приложения, ИСУПД трябва да съхранява оригиналните данни, получени от други приложения за период от време, определен от СУД	Проверка на поддържаните данни, които са прехвърлени от други приложения в уверение на това, че данните са криптирани или предпазени от увреждане, загуба или злоупотреба
	Приложението не трябва да позволява промени в лихвените	Опит за изменение на лихвен процент на изплатена вноска и

	проценти на вече изплатени погасителни вноски, а всяка промяна в лихвен процент трябва да получи и второ одобрение, за да бъде приключена	проверка дали данните не биват приети; проверка също дали приложението изисква и второ одобрение при промяна на лихвен процент
Съвместимост на стойностите	Стойността на транш трябва да е по-малка от стойността на договор	Опит да се въведе стойност на транш, която е по-голяма от стойността на договора и проверка дали данните не биват приети и дали се генерира съобщение за грешка
	Стойността при погасяване трябва да е по- ниска от стойността на емитираната ценна книга	Опит за погасяване на ценна книга на стойност по- висока от стойността на емитираната книга и проверка дали данните не биват приети и дали се генерира съобщение за грешка
	Приложението показва предупреждение за недоплатена или надплатена сума преди обработката	Симулиране на недоплащане или надплащане и проверка за предупреждение
Документи – източници	С цел гарантиране на автентичността на данните, на „входа” трябва да има проследяване към документа-източник	Подбиране на определени данни за въвеждане и проверка дали имат съответстващ

		документ-източник (напр. договор за заем, електронна поща и т.н.)
КОНТРОЛИ НА ОБРАБОТКАТА		
Целта на контролите на обработката е да се гарантира, че данните са правилно обработени в приложението и че по време на обработката няма добавени, изгубени или променени данни.		
ИЗИСКВАНЕ/ ФУНКЦИОНАЛНОСТ	**КОНТРОЛ НА ПРИЛОЖЕНИЕТО**	**ПРЕДЛОЖЕНИЯ ЗА ТЕСТВАЩИ ПРОЦЕДУРИ**
Индикация за правилното състояние	Приложението трябва да променя статута на договорите след пълното разплащане	Симулиране на приключване на разплащане и проверка дали статутът на договора се променя от „в процес на разплащане” до „изцяло разплатен”
	Приложението трябва да променя статута на ценна книга след одобрение на емитирането й	Симулиране на потвърждение за издаване на ценна книга и проверка дали статутът се променя от „неактивен” на „активен”
	Приложението трябва да променя статута на договорите или ценните книги след пълното плащане	Симулиране на финално плащане и проверка дали се променя статута на договора или ценната книга
	Приложението трябва да предвижда най-малко следните фази:	Създаване на договор, опит за извършване на разплащане във

	• Разплащане: в тази фаза се създават разплащания; • Изцяло разплатено: в тази фаза не са позволени разплащания; • Приключено: в тази фаза разплащанията не получават финансови операции, а промяната в данните не е позволена.	всяка от фазите и проверка дали данните не биват приети и дали се генерира съобщение за грешка
	Приложението трябва да съдържа правила, които правят статута на договорите (активни или неактивни) съвместими с фазите (разплащане, изцяло разплатено, погасяване, разплащане и погасяване и приключено) с цел избягване на противоречия в информацията: напр. договор, чийто статут е неактивен не може да се намира във фаза на разплащане или погасяване	Симулиране на промени в статута на договор и фазите и проверка дали те са съвместими
	Приложението трябва да съдържа програма за актуализация на фазите/ етапите на договорите: напр. когато салдото за разплащане е равно на нула, приложението следва да измени фазата от „разплащане” на „изцяло разплатено”	Симулиране на необходимите условия за промяна на фазата на договор и проверка дали промяната реално се извършва
Правилни изчисления	Приложението трябва да извършва правилни	Проверка на изчисленията чрез

	изчисления	повторно извършване; Прилагане на този тест за изчисленията към следната информация: обща стойност на дълга (договорен и секюритизиран), падеж, погасителен план (дати и стойности), стойности на комисионни, платежен поток по ценни книжа, финансова стойност на погасяване на ценни книжа и т.н.
	След промени във входящите данни, приложението трябва да актуализира данните	Внасяне на промени във входящите данни и проверка за актуализация, напр.: • Симулиране на плащане и проверка дали дължимото салдо и погасителният поток биват актуализирани; • Промяна на някои индекси и проверка дали се актуализира общата стойност на дълга.
	Приложението следва да съдържа в програмирането най- малко следните методи за изчисляване на вноските: унифицирано	Проверка на методите използвани от системата за изчисляване на вноските;

	разпределение, проста лихва, вноска, ценово приложение, приложение за постоянно погасяване, единица стойност на групирани в обща кошница валути (МБВР) и разчетна единица по валутната кошница на Интерамериканската банка за развитие (IDB)	правилността на методите може да бъде проверена чрез използване на извадка от данни
	Винаги, когато се направи промяна в полето „договорна стойност”, приложението трябва автоматично да преизчислява стойността в полето „салдо за разплащане по договор”	Промяна в полето за договорна стойност и проверка дали автоматично се внася корекция в полето за салдо за разплащане по договор
	Приложението трябва автоматично да генерира датите на вноските, като използва един от следните възможни метода: • Начална дата и фиксиран брой вноски; • Начална дата, крайна дата и брой на вноските по низходящ ред; • Начална дата, крайна дата и фиксиран брой вноски; • Начална дата и брой периоди; • Периоди	Въвеждане на необходимите данни по всеки един от възможните методи и проверка на коректността на датите на вноските
	Когато датата на вноска съвпада с неработен ден, приложението трябва да предлага два варианта:	Настройка на вноската така, че да съвпадне с неработен ден и проверка дали

	изместване на датата на следващия работен ден или на предишния работен ден	приложението предлага датата да бъде изместена или на предишния, или на следващия работен ден
	Системата следва автоматично да актуализира номиналната стойност на ценни книжа винаги когато има промяна в съответния индексатор	Промяна на индексатора на дадена ценна книга и проверка дали се актуализира съответната номинална стойност
	В случай на плащане на сума, която е по-малка от изчислената от приложението, трябва в момента на въвеждане на плащането да се показва съобщение; съобщението следва да се повтаря до датата на следващата дължима вноска	Симулиране на плащане, което е под сумата, изчислена от приложението и проверка за съобщение, както и дали съобщението се повтаря до датата на следващата вноска
	В своята база данни системата трябва да диференцира ценните книжа със симулирана емисия	Вътре в базата данни– проверка дали са разграничени симулираните ценни книжа и дали са изключени при извършване на изчисленията на общата стойност на дълга и падежа
	Когато потребител изтрие ценна книга, приложението трябва да заличи	Заличаване на ценна книга и проверка дали стойността се изтрива

	съответните стойности в базата данни	в базата данни
	Ценни книжа със статут „канцелирани" не трябва да се взимат предвид при изчисляване на дълговите ценни книжа (напр. вътрешна норма на възвращаемост, падеж и т.н.), тоест след като са канцелирани, съответните стойности следва да бъдат извадени.	Промяна на статута на ценна книга на „канцелирана" и проверка дали стойността й не се взима под внимание в изчисленията (на общата стойност, падежа и т.н.)
Подходящ контрол върху грешките в обработката	Приложението следва да третира по различен начин погасителни вноски със просрочено плащане	Проверка дали приложението изчислява правилно всички промени по просрочените вноски
	Грешки в обработката от преди дни/седмици назад не бива да остават неотстранени	Проверка дали има критерии относно броя дни, необходими за отстраняване на грешки в системата, проверка за съобщения за грешки и обсъждане с лицата, отговорни за системата/ управлението на дълга мерките, необходими за коригиране на неизправностите
	В случай на грешка в обработката, приложението трябва да канцелира обработката и да съхрани в базата с данни датата, времето и техническата	Симулиране на грешка в обработката и проверка дали приложението архивира в

	причина за възникналия проблем	базата с данни датата, времето и техническата причина за възникналия проблем
Правилно записване	Приложението трябва да дава възможност на управителите на дълга акуратно да записват паричните потоци (свързани със заеми в чуждестранна и местна валута, дейности по търгуване и хеджиране, гаранции и предоставяне на заеми със заемни средства) за всички транзакции	Извършване на транзакция и проверка дали съответстващият запис е правилен и точен
	Приложението следва да съхранява историята на транзакциите, извършени по време на срока на действие на договора и да включва подробности относно кредитора, договорната стойност и датата на приключване на проекта, както и крайни дати за разплащания	Проверка дали историята на транзакциите, които се отнасят до дадена ценна книга или договор съответства на архивираната информация по дълга
	Приложението трябва да разполага с автоматично стартиране на задачи в графиците зададени от СУД за актуализиране на индекси, общ дълг и т.н.	Проверка на автоматичното стартиране, както и дали този процес работи добре
	За определен вид ценни книжа, чиято	Създаване на ценна книга с еднаква

Верен график на задачите	амортизация/погасяване се извършва със същата честота както лихвата (цена, например), системата трябва да гарантира, че и лихвата, и амортизацията имат еднакъв график на плащанията	честота по отношение на амортизацията и лихвата и проверка дали имат еднакъв график на плащанията
	Трябва да се поддържа одитната следа на ИСУПД, която да дава възможност за проследяване на договор за дълг и дългова ценна книга от подписването/ емитирането до изплащането	Проверка на одитната следа на извадка от договори и ценни книжа от подписването/ емитирането до изплащането
КОНТРОЛИ НА „ИЗХОДА”		
Целта на контролите на „изхода” е да се гарантира интегритета на изходящите данни и коректното и навременно разпределение на генерирания резултат.		
ИЗИСКВАНЕ/ ФУНКЦИОНАЛНОСТ	**КОНТРОЛ НА ПРИЛОЖЕНИЕТО**	**ПРЕДЛОЖЕНИ ТЕСТОВИ ПРОЦЕДУРИ**
Контрол върху потребителите на информацията	Приложението трябва да има архив/регистър със записани имена на потребителите, които са поискали доклади, както и датите и времето на исканията	Искане на определени доклади и проверка дали приложението записва исканията
	Приложението трябва да изисква специално разрешение за зареждане на определени доклади (по-конкретно доклади, които съдържат поверителна информация)	Опит за получаване на такива доклади

Своевременно и надеждно докладване	Приложението следва да генерира предварително зададени доклади (класификации на облигации, заеми и траншове, напр. падеж, статус, финансови източници, тип финансиране, кредит, вид инструмент, условия, неплатени полици и т.н.)	Опит за получаване на някои предварително зададени доклади
	Приложението следва да изготвя доклади по правилния начин, като гарантира пълнотата и интегритета на информацията	Проверка дали докладите се изготвят съобразно условията за ползване; Проверка дали докладите съдържат номера на страниците и общ брой; Прилагане на този тест спрямо следните доклади: доклад за матуритет (за договорен и секюритизиран дълг), доклад за непогасено салдо, и т.н.
	Приложението следва да позволява докладване, както глобално (всички дългови ценни книжа), така и конкретно, като напр.: • По статус на ценните книжа (емитирани, канцелирани, обратно изкупени и т.н.);	Опит за генериране на доклади, глобални и конкретни, като за критерий се използват следните данни: • статус на ценните книжа (емитирани, канцелирани, обратно изкупени

	• За събития в определен времеви отрязък (емисии, обратно изкупуване и т.н) • По краткосрочни и дългосрочни акции; • По позиции в портфейла; • По видове ценни книжа; • По интервал на падежа	и т.н.); • събития между определени дати (емисии, обратно изкупуване и т.н); • краткосрочни и дългосрочни акции; • вид ценна книга; • интервал на падежа
	Докладите следва да представят цялостна и вярна информация	Генериране на доклади и повторно извършване на изчисленията; Прилагане на този тест спрямо следните доклади: доклади за матуритет (за договорен и секюритизиран дълг), доклад за непогасено салдо и т.н.
	Докладите трябва да представят абсолютно същата информация като тази, която излиза на екраните на приложението	Сравняване на доклади за съответствие на информация с информацията от екраните на приложението; Прилагане на този тест спрямо следните доклади: доклади за матуритет (за договорен и секюритизиран дълг),

		доклад за непогасено салдо и т.н.
	Трябва да има съответствие между стойностите представени в Доклада за матуритет, Доклада за непогасено салдо и Доклада за акциите	Сравняване на тези доклади за последователност
	Системата трябва да може да изготвя доклади за общите стойности на дълга на индивидуална и обобщена основа заедно с прогнозиране относно обслужването на дълга и бъдещите заеми и ценни книжа	Опит за получаване на такива доклади; Проверка дали докладите включват както съществуващи, така и очаквани дългови операции
	Приложението трябва автоматично да генерира доклади за дневния финансов график на всички активни договори; трябва също да позволява ръчно генериране на доклади по конкретни договори	Проверка за генериране на автоматични доклади по всички активни доклади и опит за ръчно генериране на доклади по конкретни договори
Правилно прехвърляне на данни	Прехвърлянето на данни между приложенията, етапите на обработка или и двете трябва да бъде точно и пълно	Симулиране на прехвърляне на данни между приложения и проверка за точност и пълнота на данните
Полезни съобщения на „изхода”	Когато потребител поиска достъп до приложение, то трябва да покаже съобщение със следната информация:	Влизане в приложението и проверка дали показва всички тези съобщения

	• договори с падеж в следващите 5 дена; • договори с просрочено плащане на вноските; • договори с частично плащане на вноските; • договори с просрочени дати за разплащане; • договори с крайни срокове за разплащане от 5 дена (приложението трябва ежедневно да изпраща съобщения докато се извърши разплащането, стойността на разплащането бъде канцелирана или крайният срок бъде променен	
	Приложението трябва да показва какъв е статусът на изчисленията: или „текущо изчисляване”, или „приключено изчисляване”	Искане за извършване на изчисление и проверка дали приложението показва статусът на операцията
	В края на генерирането на доклад, приложението трябва да покаже съобщение, че генерирането на доклад е приключено, или да покаже искания доклад	Искане на доклад и проверка дали приложението показва съобщение, че операцията е приключена, или показва искания доклад
	Приложението трябва да укаже какъв е статуса на генерирания доклад – „в процес на изпълнение” или	Генериране на доклад и проверка дали приложението показва какъв е

	„приключен”	статуса на операцията
	Ако има промяна в лихвените проценти, приложението трябва да покаже предупреждаващо съобщение	Промяна на лихвените проценти и проверка за предупреждаващо съобщение
	Преди обработката на канцелиране или обратно изкупуване на ценни книжа, приложението трябва да покаже екран с информацията, която ще се заличава, така че потребителят да потвърди операцията	Опит за обратно изкупуване или канцелиране на ценни книжа и проверка дали приложението показва съобщение, че потребителят трябва да потвърди операцията

ФИГ. 1: ОДИТИ НА ПУБЛИЧЕН ДЪЛГ, ИЗВЪРШЕНИ ОТ ВОИ НА БРАЗИЛИЯ

Одит на интегрираната система относно дълга (ИСД), извършен през 2014 г. от Сметната палата на Бразилия към федералното правителство на Бразилия

Като взе предвид, че се провежда тестване на ИСД относно вътрешния секюритизиран дълг, одитният екип реши да се концентрира единствено върху тестване на процесите, свързани с управление на външния дълг (секюритизиран идоговорен). Стигна се до следните одитни наблюдения и констатации:

Стратегия и общо управление на ИТ системата

Съгласно *Оперативния наръчник*, с цялостното въвеждане на ИСД на разположение ще бъдат следните функции:

а) голямо разнообразие от функции за изчисления, като актуализирана номинална стойност, единична цена, обща стойност (както на секюритизирания дълг, така и на договорните дългови задължения), финансово планиране на договорите и договорно и облигационно ценообразуване и падежи;

б) разнообразни функции за търсене и докладване, както по отношение на регистриране на данни, така и резултати от изчисления;

в) финансови операции, сред които издаване на облигации, погасяване на договорни задължения, обратно изкупуване и прехвърляне и т.н.; и

г) информационен регистър, който се използва в пълна степен в различните бизнес модули

По отношение на стратегията и общото управление на ИТ системата, основните наблюдения и одитни констатации са както следва:

- Няма програма за обучение по най-широко използваните системи за управление на публичния дълг, Сеорфи и ИСД;
- Няма очаквана дата на цялостно въвеждане на ИСД, което включва и вътрешния секюритизиран дълг;
- Някои важни операции, като задействане на договор, погасяване, обратно изплащане, промяна в лихвените нива или в договорени стойности, се извършват от един-единствен човек. Не е необходимо одобрение или двойно оторизиране в системата. Сигурността на операциите зависи единствено от адекватността на профила, което поражда проблем във връзка с разделянето на задълженията;
- Друг проблем относно разделянето на задълженията е недостига на служители за разработване на ИСД; разработват я служители на СУД, едновременно с изпълнение на редовните си служебни задължения;
- Оценката на уязвимостта на операционните рискове в ИТ процесите е готова, но липсва оценка за смекчаване на тези рискове;

Контроли на сигурността и околната среда

По отношение на контролите на сигурността и околната среда, основните наблюдения и одитни констатации са както следва:

- СУД не е назначил Ръководител по информационна сигурност и комуникации, а Комитетът по информационна сигурност, който отговаря за назначаването на ръководителя, не е започнал да работи да ефективно;
- Няма официален ПНД, а работните процеси във връзка с управлението на публичния дълг са в процес на преглед с цел изготвяне на ПНД;
- Анализът, извършен от одитния екип отбелязва наличието на трима активни генерични потребителя, което възпрепятства добрите ИТ практики, основаващи се на точка 11.2.1 от ISO / IEC 27002: 2005, където се препоръчва ползването на уникален потребителски идентификатор, за да се гарантира отчетността по отношение на всеки потребител на системата;
- Независимо, че дефинирането на достъпа до ИСД следва да се направи единствено посредством А3 цифров сертификат и достъпът чрез национален идентифициращ номер и парола следва да бъде изключение, анализът на базата на данни с потребители на ИСД показва, че не е заложен краен срок за действие на изключението;
- Анализът на базата на данни с потребители на ИСД показва пропуски в процеса за преглед на достъпа на потребителите;
- Одитният екип установи пропуски и в ежедневната рутинна автоматична поддръжка на базата данни с потребители на ИСД;
- ИСД не прави запис на одитната следа за повечето от транзакциите, като в резултат СУД не провежда периодичен преглед на одитните следи генерирани от системата, както и не осъществява мониторинг върху транзакциите в ИСД;
- ИСД не притежава одитна функция, която обичайно генерира, съхранява и анализира системния регистър;
- Одитният екип забеляза отсъствие на тестови план и свързаните с него резултати в системите с най-широка употреба в СУД – Сеорфи и ИСД;
- Одитният екип не получи потвърждение, че е създаден екип за реагиране на инциденти в компютърните мрежи, който да отговаря за получаване на информация, преглед и реагиране на инциденти в областта на сигурността;
- Одитният екип забеляза отсъствие на план за непрекъснатост на ИТ услугите, който под формата на официален документ описва непрекъснатостта на всички ИТ услуги, управлявани от съответната агенция или организация;

Оперативни контроли и документация

По отношение на оперативните контроли и документация, основните наблюдения и одитни констатации са както следва:

- Интерфейсът не е особено лесен, заради което потребителите на ИСД следва да притежават повече предварителни познания за системата;
- Няма наръчник за потребителя на ИСД;
- Скоростта на обработка на необходимите изчисления е ниска. Това прави невъзможно едновременното генериране на изчисления и доклади. Тъй като има множество едновременни потребители на системата, този проблем би могъл да намали ефективността на системата. Одитният екип предложи СУД да прецени евентуални подобрения с цел повишаване на обработващия капацитет на системата;

Контроли на приложенията

След като одитният екип проведе контролни тестове на входа, обработката и на изхода на ИСД за външния държавен дълг, одитните констатации и наблюдения са както следва:

- Много от съобщенията за грешка са неясни, а понякога не се показват пред потребителя.
- По време на тестове на контролите на „входа" на приложението одитният екип установява няколко съобщения за грешки, които не обясняват причината за грешката.
- По време на тестове на контролите на приложението за обработката относно външния договорен дълг, одитният екип установява различия в стойностите на финансовия доклад за паричните потоци.
- При тестове на контролите на приложението на „изхода", одитният екип установява, че ако въведените данни не са коректни, приложението не генерира някои доклади относно договорения дълг, съгласно очакваното, като приложението не идентифицира грешка пред потребителя.
- По време на тестове на контролите на приложението на „изхода", одитният екип идентифицира грешки в докладите за договорния дълг заради използваните в системата остарели индекси.
- Някои доклади за договорен дълг съдържат непълна информация.

Препоръки

Въз основа на одитните констатации и наблюдения, одитният екип препоръчва в рамките на 90 дена Националният секретариат на държавната хазна да разработи план за действие, който включва график за изпълнение на следното:

- Определяне на очаквана дата за цялостно внедряване на ИСД, в това число и вътрешен секюритизиран дълг;
- Назначаване на Ръководител по информационна сигурност и комуникации и Комитет за информационна сигурност;
- Официализиране на ПНД;
- Официализиране на План за непрекъснатост на ИТ услугите;
- Създаване на екип за реагиране на инциденти в компютърните мрежи;
- Оценка и смекчаване на оперативните ИТ рискове;
- Преглед на рутинната ежедневна автоматична поддръжка на базата данни с
  потребители на ИСД;
- Преглед на процеса за преглед на достъпа на потребителите на ИСД;
- Преглед на процеса за предоставяне на достъп на общите потребители на ИСД;
- Установяване на процедури за периодичен преглед на одитните следи, генерирани от ИСД;
- Предоставяне на архива на записите на приложението на ИСД;
- Преглед на съобщенията за грешка в ИСД;
- Разработване на ръководство за потребители на ИСД;
- Преглед на рутинното докладване на ИСД.

ФИГ. 2: ОДИТИ НА ПУБЛИЧЕН ДЪЛГ, ИЗВЪРШЕНИ ОТ ВОИ НА МОЛДОВА

Оценка на контролите на приложението, извършена от Сметната палата на Молдова

Приложението СУДФА притежава достатъчно интегрирани контроли, които автоматично проверяват дали въвеждането на данни е правилно изпълнено. Обаче има някои аспекти, които будят тревога и следва да бъдат решени: операторите могат да въвеждат данни в класификаторите на приложението и в други системни таблици, които могат да повлияят върху точността и интегритета на данните посредством дублиране или заличаване на регистрации.

Препоръка № 15: Да се преразгледат правата на операторите за въвеждане, промяна или заличаване на данни в класификатора на базата данни на СУДФА, или да се идентифицират операциите, които водят до дублиране на данни или грешни въвеждания.

Освен стандартните доклади в приложението СУДФА, голям брой общи доклади се разработват в Excel. Не всички видове доклади се използват системно.

Повечето от изискуемите доклади се изготвят в Excel. Обаче има определени доклади, които се генерират ръчно от данни, получени от други доклади.

Безпокойство предизвиква обновяването на данни в докладите в Excel.

Генерирането на доклади е сложна процедура, която може драстично да бъде повлияна от човешки грешки. Нещо повече, генерираните доклади могат да бъдат променяни без разрешение, а такива грешки могат да се появят и в други важни обобщаващи доклади, при които сигурността трябва да е максимална и които представляват основната дейност на Главната дирекция по публичен дълг.

В резултат, някои малки пропуски биха могли да имат драматичен ефект върху надеждността и точността на данните във важните доклади за дейността на Главната дирекция по публичен дълг.

Препоръка № 16: Да се обмисли оптимизирането или автоматизирането на процеса за промяна на докладите, които се генерират. Да се определи начин за автоматично генериране на обобщаващи доклади, като се елиминира вероятността за човешка грешка. Да се обмисли възможността за преминаване към версия 6.0.

БИБЛИОГРАФИЯ

Азиатска организация на Върховните одитни институции. Изследователски проект. *Указания за ИТ одити – 6mo издание*. септември 2003 г.

Галегос, Фредерик, Сандра Сенфт, Даниъл П. Мансън и Карол Гонзалес. *Контрол и одит на информационни технологии*. Издателство Ауербах. САЩ 2004 г.

Служба на главния контрольор и одитор на Индия. *Одит на информационни технологии – общи принципи* (серия от монографии по ИТ одит # 1).

Международен валутен фонд и Световна банка. *Указания за управление на публичен дълг*, 1 април, 2014 г.

Международна организация на Върховните одитни институции. МСВОИ 300 Принципи на одит на изпълнението. Септември 2019 г.

Международна организация на Върховните одитни институции. МСВОИ 3000, *Стандарт за одит на изпълнението. Септември* 2019 г.

Международна организация на Върховните одитни институции. МСВОИ 5310, *Методология за преглед на сигурността на информационните системи*. октомври 1995 г.

Инициатива на ИНТОСАЙ за развитие. РГОИТ, *Наръчник на ИИР по ИТ одити за Върховни одитни институции*. февруари 2014 г.

Паркър, Ксения Лий. *Одити на информационни системи*. CCH Incorporated. САЩ 2006 г.

Департамент по вътрешна сигурност на САЩ – интернет страница: http://www.dhs.gov.

Държавна служба на САЩ по отчетност. *Ръководство за одити на контроли на федерални информационни системи (FISCAM)*. GAO-09-232G. февруари 2009 г.