30 листопада 2015 року

# Резюме
# спільних висновків та рекомендацій міжнародного координованого паралельного аудиту інформаційних систем управління державним боргом

Упродовж 2013-2014 років вищі органи фінансового контролю Бразилії, Болгарії, Фіджі, Грузії, Молдови, Румунії, України, Ємену та Замбії (далі – ВОФК-учасники) провели міжнародний координований паралельний аудит інформаційних систем управління державним боргом відповідно до Стратегічного плану робочої групи INTOSAI з державного боргу (WGPD). ВОФК Китаю, Єгипту, Мексики і Російської Федерації брали участь у проекті як спостерігачі.

Цей аудит був проведений на основі Загальної програми паралельного аудиту [1], розробленої в 2012 році Рахунковою палатою України (координатор паралельного аудиту), відповідно до Міжнародних стандартів вищих органів фінансового контролю (ISSAI) і кращих національних практик. Резюме національних аудиторських звітів, які підготовлені ВОФК-учасниками в рамках паралельного аудиту, доповнюють спільний звіт про результати паралельного аудиту.

Під час паралельного аудиту оцінювалася ефективність функціонування інформаційних систем управління державним боргом (ІСУДБ), які функціонують у межах юрисдикцій ВОФК-учасників. Основна мета аудиту полягала у відповіді на такі питання:

- Чи належним чином здійснювалися процеси управління національними інформаційними системами управління державним боргом та контролю за ними?

- Чи мають досліджувані інформаційні системи адекватний загальний та прикладний контроль і чи був він належним чином реалізований?

Паралельний аудит показав, що державні органи створили надійні та стійкі ІСУДБ разом з відповідною інфраструктурою; системи були розроблені і підтримувалися на сучасному технічному рівні. В цілому, розглянуті інформаційні системи забезпечили збір, оброблення та надання звітних даних щодо боргу, а також ведення справ у системі відповідно до національних вимог та очікувань користувачів щодо можливостей системи, що сприяло полегшенню процесу управління державним боргом. Разом з тим аудит виявив деякі недоліки і слабкі сторони у питанні загального управління, загальних і прикладних засобів контролю, пов'язаних з інформаційними системами боргу.

Загальне управління ІСУДБ не було достатньою мірою впорядковано, щоби забезпечувати безперервний розвиток систем відповідно до загальних стратегічних цілей установи. Більшість з підрозділів управління боргом (ПУБ), які перевірялися, не

[1] Затверджена ВОФК-учасниками паралельного аудиту за результатами установчого засідання, що відбулося у квітні 2013 року в м. Києві, Україна.

мали затвердженої стратегії розвитку ІСУДБ. Навіть якщо загальна стратегія розвитку ІТ існувала, вона не була оновлена відповідно до бізнес-процесів установи, в якій проводився аудит. Інтеграція ІСУДБ в єдину інформаційну систему фінансового управління не виконана. Майже ніде ІСУДБ не була повністю інтегрована до фінансових/бюджетних систем управління. Крім того, немає планів управління проектами або інших офіційних документів, на підставі яких буде здійснюватися розвиток системи.

Окремі підрозділи з управління боргом використовували місцеві (самостійно розроблені) системи, зокрема для внутрішнього державного боргу, які не були пов'язані із загальною системою управління боргом та фінансового аналізу (DMFAS), і навіть були несумісними між собою. Не охоплений весь процес і вся робота в контексті повної автоматизації бізнес-процесів з управління державним боргом. У багатьох підрозділах управління боргом аудитори помітили нечіткий розподіл функцій і обов'язків між персоналом управління боргом на технічному рівні. Крім того, вони повідомили про непоодинокі випадки, коли права доступу і права на підтвердження оплати не були належним чином відокремлені.

Оцінка ризику як виявлення можливих слабких сторін, які можуть скомпрометувати ІСУДБ, не проводилася. Підрозділи управління боргом майже не використовували спеціалізовані розробки для оцінки ризику апаратної, програмної та комунікаційної інфраструктури. Не проводився внутрішній аудит ІСУДБ як засіб посилення ІТ-контролів у системі. Навчання персоналу здійснювалося лише за потребою, але без програми систематичного навчання.

Управління безпекою та контроль середовища ІСУДБ були в стані, що підтримує загальні бізнес-процеси управління боргом. Разом з тим низка установ не мала затвердженої політики безпеки ІСУДБ. Фізичний доступ до файлів і ІТ-обладнання переважно добре контролювався. За винятком поодиноких випадків, сервери мали достатню інфраструктуру і захист. У той час як в окремих юрисдикціях доступ до файлів і баз даних передбачав кілька рівнів захисту, контроль доступу до програм і важливих даних у багатьох установах управління боргом не був належним чином забезпечений. Деякі ІСУДБ працювали без оновленого антивірусного програмного забезпечення. Схеми захисту паролем були погано розроблені. Навіть якщо паролі користувачів мали дату закінчення, в деяких випадках паролі були слабо захищені від несанкціонованого доступу.

Аудит виявив слабкість планування безперервності ІТ-послуг, зокрема, через відсутність плану безперервності бізнес-процесів (ПББП) плану відновлення після катастроф (ПВК) або його погану узгодженість. Деякі ПУБ розробили внутрішні правила щодо забезпечення безпеки інформаційних ресурсів через регульований фізичний доступ, захист інформаційної системи від пошкоджень, стихійних лих та/або втручання людини і резервування інформації. У деяких випадках звіти про інциденти стосовно безпеки були слабкими або не існували взагалі. Політику створення резервної копії (частота і режим резервного копіювання, тип резервного копіювання, зберігання інформації та її розташування) не передбачено в багатьох установах.

Операційний контроль і документація відповідали місцевим вимогам із оброблення даних щодо боргу. ІСУДБ, як правило, мали достатній рівень контролю для захисту бази даних боргу від несанкціонованого доступу. Але багато розроблених на місцевому рівні ІСУДБ не забезпечували ведення журналу реєстрації своїх операцій. У двох випадках ПУБ деактивували журнал реєстрації. Будь-які компенсаційні механізми для забезпечення підзвітності та відстеження операцій не були встановлені. Відсутність довідкової служби для забезпечення безперебійної допомоги при виникненні проблем також виявлено в багатьох установах.

Як правило, прикладні засоби контролю були наявні та зазначені в керівництві для контролю. Аудит засвідчив наявність ряду встановленого вхідного контролю для захисту ІТ-інфраструктури та комп'ютерних програм. Вхідний контроль був належним, що знижувало ризик помилки або шахрайства. Однак у деяких ІСУДБ спостерігалися дублювання вхідних даних щодо боргу, а кількість дублюючих операцій залишилася невизначеною. Виконавши тести обробки контролю щодо однієї з ІСУДБ, аудитори виявили, що багато повідомлень про помилки не були чіткі, а іноді такі повідомлення взагалі не відображалися на екрані до уваги користувача. Крім того, виявлена відсутність функції для переривання сеансу користувача після закриття, а потім відкриття Інтернет-браузеру. Шляхом тестування прикладного вихідного контролю аудитори також помітили деякі недоліки.

Беручи до уваги спостереження та висновки паралельного аудиту, ВОФК-учасники надали такі ключові рекомендації для відповідних національних урядів:

- розробити/оновити стратегію ІСУДБ, яка заснована на правилах оцінки ризику і відповідала б бізнес-процесам установи, забезпечуючи її поступову інтеграцію до відповідних фінансових і бюджетних інформаційних систем управління;
- забезпечити посилення політики безпеки та процедур контролю доступу ІСУДБ, у тому числі належне планування безперервності бізнес-процесів і розподілу обов'язків серед персоналу з управління боргом і співробітниками, які виконують адміністрування системи;
- підвищити потенціал ІСУДБ, впроваджуючи надійні функціональні та прикладні засоби контролю поряд із забезпеченням належного внутрішнього аудиту і створенням служби технічної підтримки.