

Івахненко С.В.,

кандидат економічних наук,
доцент кафедри фінансів Національного університету
“Києво-Могилянська Академія”

НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗАЦІЇ КОРПОРАТИВНОГО ФІНАНСОВОГО КОНТРОЛЮ: СВІТОВИЙ ДОСВІД

Розглянуто нормативні акти в галузі корпоративного фінансового контролю. Проаналізовано світовий досвід регулювання процесів внутрішнього фінансового контролю в корпораціях, у т. ч. в умовах застосування інформаційних технологій. Запропоновано шляхи нормативного регулювання й адаптації нормативних актів в Україні.

Normative documents in the field of the corporate internal control are considered in the article. World experience of adjusting the processes of internal control is analyzed including the environment of the IT application. Ways of the normative adjusting and adaptation of the normative acts in Ukraine are offered.

Позитивні тенденції останніх років у економіці країни та зростання конкуренції практично в усіх галузях засвідчили, що Україна перейшла на якісно новий рівень ведення бізнесу. На цьому рівні ринок досягає насиченості, а управлінців-власників змінюють наймані управлінці, які мають спеціальну освіту та можуть забезпечити підприємству стабільний розвиток у довгостроковій перспективі. Іншою тенденцією є укрупнення бізнесу. Компанії, які починали свою діяльність як приватні підприємці чи приватні підприємства, розвиваються, виростаючи до акціонерних товариств. За таких умов, особливо якщо представництва чи філії компанії знаходяться в різних регіонах або навіть у різних державах, великого значення набувають налагодження системного підходу в управлінні та уніфікація бізнес-процесів, системний підхід до корпоративного фінансового контролю.

Компанії, які впроваджують систему внутрішнього контролю, мають знайти оптимальне поєднання контрольних процедур та ефективності ведення бізнесу, адже надмірний акцент на контрольних процедурах не дає можливості підприємству займатися власне бізнесом. Разом із тим контрольні процедури повинні постійно тестуватися і вдосконалюватися.

Початок нового тисячоліття відзначився низкою корпоративних скандалів у США та Європі, найгучнішим із яких було банкрутство американської компанії “Енрон”. Наслідком цього стало підписання 30 липня 2002 року Президентом США Дж. Бушем Закону Сарбейнса-Окслі (*Sarbanes-Oxley Act of 2002*), який установив низку вимог щодо внутрішніх контрольних процедур, що передують складанню фінансової звітності для всіх публічних компаній. Це справило значний вплив не лише на американські компанії, а й на всі компанії, які розміщують свої

акції на американських фондових біржах — дотримання вимог Закону Сарбейнса-Окслі стало обов'язковою умовою для лістингу на біржі.

На сьогодні в Україні немає законодавчого регулювання системи внутрішнього контролю підприємств на зразок згаданого закону, проте в конкурентній боротьбі за нових акціонерів переможуть ті компанії, яким вдасться переконати майбутніх власників у ефективності системи корпоративного фінансового контролю.

Метою статті є аналіз існуючих у світі нормативних актів у галузі внутрішнього корпоративного контролю та вироблення оптимальної схеми нормативного регулювання питань корпоративного фінансового контролю в Україні.

Беззаперечним світовим лідером щодо уваги до систем внутрішнього контролю корпорацій є США. Зауважимо, що саме прийняття Закону Сарбейнса-Окслі, який суттєво змінив і продовжує змінювати не лише американську, а й світову бізнес-практику, спричинило появу подібних нормативних актів в інших країнах. Проте нерозуміння вимог цього закону є однією з причин того, що дуже обмежена кількість українських компаній здійснюють початкове розміщення акцій (*initial public offering*) на американських біржах. Українські компанії використовують для цього інші біржі, зокрема Лондонську фондову біржу, таким чином обмежуючи собі доступ до потенційних інвестицій.

Однією з причин нерозуміння українськими компаніями положень Закону Сарбейнса-Окслі є практично повна відсутність публікацій українською мовою, де б висвітлювались питання щодо його застосування. Йдеться як про журнальні публікації, так і книги та розділи у книгах. Українські науковці лише іноді мимохідь згадують про цей закон. Зокрема, голова Федерації бухгалтерів і аудиторів України Сергій Голов зазначає, що Закон Сарбейнса-Окслі ввів у США персональну відповідальність генерального й фінансового директорів за недостовірність фінансової звітності¹.

Деяка інформація російською мовою міститься у відкритих звітах аудиторських фірм із “великої четвірки”, наприклад, короткий огляд закону фахівцями фірми “Ернст енд Янг”². Натомість практики й науковці США всебічно розглядають проблеми його застосування як у практичному, так і науковому аспектах. Зокрема, велика кількість матеріалів і статей, корисних для аудиторів, містяться на web-сайті www.audit.net. Проте найбільший інтерес становлять спеціалізовані книги: наприклад, посібник американських авторів Дж. Тібодо і Д. Фраєр³ чи ґрунтовний підручник Гр. Роджерса⁴ тощо. Усі ці публікації є важкодоступними в Україні.

Поряд з регламентацією внутрішніх контрольних процесів корпорацій Закон Сарбейнса-Окслі регламентує діяльність незалежних аудиторів, покликаних

¹ Голов С. Управлінський облік як фактор підвищення якості корпоративного управління // Податкове планування. — 2005. — № 5. — С. 41—50.

² <http://www.ey.com>.

³ Thibodeau J., Freier D. Auditing After Sarbanes-Oxley. — McGraw-Hill., 2006. — 288 p.

⁴ Rogers Gr. Financial Reporting of Environmental Liabilities and Risks after Sarbanes-Oxley. — Wiley, 2005. — 408 p.

підтверджувати інформацію, яку компанії надають у фінансовій звітності. У цій галузі нормативи закону спрямовані на підвищення рівня незалежності аудиторів для забезпечення об'єктивності й вірогідності аудиторських висновків. Закон також безпосередньо стосується консультаційних послуг аудиторських фірм, зокрема з питань налагодження системи внутрішнього контролю компаній.

У світі існує також значний набір підзаконних актів і стандартів, прийнятих у розвиток існуючих законів з питань внутрішнього контролю. Наприклад, міжнародні стандарти аудиту вимагають від зовнішніх аудиторів розуміння бізнес-процесів компанії-клієнта, у т. ч. того, як ці процеси ініціюються, реєструються, обробляються і контролюються. Це необхідно аудиторам як для оцінки ризиків контролю при формуванні аудиторського висновку щодо фінансової звітності, так і для надання консультацій. А оскільки бізнес-процеси переважної більшості компаній залежать від інформаційних технологій, то програмні й технічні компоненти інформаційних систем займають найважливіше місце при здійсненні внутрішнього контролю у процесі формування фінансової звітності. Однак, окрім згаданих стандартів, інші нормативні документи українським фахівцям практично недоступні.

Незважаючи на важливість цих питань, наукових і практичних публікацій українською та російською мовами із застосування інформаційних технологій при запровадженні на підприємствах нормативів внутрішнього контролю немає. Є лише певна рекламна інформація деяких фірм — розробників програмного забезпечення, які стверджують, що їхні програмні продукти містять відповідні можливості. Це, наприклад, місцева філія фірми SAP AG (www.sap.com) та російська фірма Терра-Лінк.

Сучасні світові нормативи, які стосуються корпоративного фінансового контролю, мають доволі тривалу історію розвитку. Так, велика депресія 1929—1933 років висвітлила слабкі місця в організації публічних компаній, а також показала небезпеку безконтрольного підходу до формування вартості корпоративних цінних паперів. Сполучені Штати опинилися в епіцентрі депресії, тож уряд був змушений вжити відповідних заходів, зокрема у 1933—1934 роках було прийнято закони, які мали на меті відновити довіру інвесторів і стали фактичною основою для вироблення загальноприйнятих у країні принципів бухгалтерського обліку (*General Accepted Accounting Principles*). Закон 1933 року (*Securities Act of 1933*) установив перелік обов'язкових вимог для первинної емісії цінних паперів (акцій та облігацій). Закон 1934 року (*Securities Exchange Act of 1934*) стосувався вторинного ринку цінних паперів і містив вимоги до компаній, цінні папери яких продавалися на відкритих фондових торгах чи спеціалізованих ринках. Згідно з цим законом було створено Комісію з цінних паперів і біржових операцій (*Securities and Exchange Commission — SEC*), яка отримала право й відповідальність установлювати стандарти фінансової й бухгалтерської звітності для компаній, цінні папери яких виставлено на відкриті торги (*public companies*).

Як уже зазначалося, прийняття Закону Сарбейнса-Окслі стало новим етапом у розвитку корпоративних систем внутрішнього контролю. Одним із найвідоміших

розділів цього закону став параграф 404, згідно з яким менеджмент корпорації, представленої на фондових ринках, зобов'язаний створити ефективну систему внутрішнього контролю. Цей розділ містив вимогу з проведення контрольних процедур щодо оцінки ефективності внутрішньої системи контролю з боку незалежних аудиторів. Такі заходи стали не лише найбільш жорсткими по відношенню до американських корпорацій, починаючи з 30-х років XX століття, але й принесли значні додаткові витрати підприємствам.

Важливою історичною подією щодо корпоративного внутрішнього контролю стало створення у США в 1985 році Комітету спонсорських організацій Комісії Тредуя (*Committee of Sponsoring Organizations of the Treadway Commission — COSO*). Метою його створення була підтримка Національної комісії з питань шахрайств при складанні фінансової звітності (*National Commission on Fraudulent Financial Reporting*) — незалежної приватної організації, яка вивчала фактори, що спричиняли шахрайства при підготовці фінансової звітності, та готувала рекомендації для публічних компаній, їхніх незалежних аудиторів, SEC та інших інституцій, а також для навчальних закладів. До складу Комісії входять аудитори, представники бізнесу, інвестиційних компаній та Нью-Йоркської фондової біржі. Важливим результатом роботи комітету COSO стало напрацювання у 1992 році “Інтегрованої (концептуальної) основи внутрішнього контролю” (*Internal Control Integrated Framework*), яка в редакції 1994 року й досі використовується як база для оцінки корпоративних систем внутрішнього контролю у США згідно із Законом Сарбейнса-Окслі (параграф 404).

Документ COSO надає визначення внутрішнього контролю, опис його компонентів, наводить критерії оцінки контрольних систем корпорацій та методики для складання звітів по системах внутрішнього контролю, а також матеріали, котрі керівники, аудитори тощо можуть використовувати для оцінки таких систем. Головні цілі документа — ввести загальне визначення внутрішнього контролю, яке влаштовувало б різні задіяні сторони, та запропонувати стандарт, за яким організації можуть оцінити й визначити шляхи вдосконалення систем контролю.

У документі наголошується, що система внутрішнього контролю — це інструмент, а не замітник управління, і що засоби контролю повинні бути вбудовані в операційну діяльність (а не побудовані на її базі). Хоча внутрішній контроль тут слушно визначено як процес, оцінку ефективності внутрішнього контролю рекомендовано проводити на певний момент часу. COSO визначає внутрішній контроль як процес, здійснюваний радою директорів компанії, менеджментом, іншим персоналом, для забезпечення розумної гарантії досягнення таких цілей:

- ефективність та економічна доцільність операцій;
- надійність фінансового звітування;
- узгодженість із відповідними законами та нормативами.

Досягати цього запропоновано шляхом спостереження за такими компонентами внутрішнього контролю: 1) середовище контролю; 2) оцінка ризику; 3) контрольні заходи; 4) інформація та комунікація; 5) моніторинг.

Середовище контролю забезпечує основу для інших компонентів, адже зачіпає такі чинники, як філософія менеджменту й стиль керівництва, правила і прийоми роботи з трудовими ресурсами, моральні чесноти працівників, організаційна структура, а також керівна роль ради директорів.

Оцінка ризику поділяється на ідентифікацію ризиків та їх аналіз. Ідентифікація ризику включає розгляд зовнішніх чинників, таких як технологічне зростання, конкуренція, зміни в економіці, а також внутрішніх, таких як кваліфікація персоналу, природа діяльності компанії, характеристики функціонування інформаційної системи. Аналіз ризиків зачіпає оцінку значущості ризику, вірогідність виникнення ризику і розгляд питань управління ризиком.

Контрольні заходи містять норми і процедури, які забезпечують виконання працівниками директив керівництва, та охоплюють перегляд системи контролю, розподіл обов'язків і засоби контролю інформаційної системи. Засоби контролю інформаційних систем поділяються на загальні й прикладні. Загальні охоплюють права доступу, програмне забезпечення й розвиток системи, прикладні запобігають помилкам під час упровадження системи або знаходять і коригують існуючі в системі помилки.

COSO розглядає як інформацію, так і комунікації. Щодо інформації переглядає потреби фіксувати відповідну внутрішню й зовнішню інформацію, потенціал стратегічних та інтегрованих систем, а також вимоги до якості даних. Опис комунікацій фокусується на передачі інформації з питань внутрішнього контролю, а також зборі конкурентної, економічної та законодавчої інформації.

Моніторинг системи контролю керівники здійснюють шляхом перегляду результатів контрольних заходів і шляхом проведення спеціальних оцінок. Стандартні контрольні заходи включають, наприклад, порівняння наявних активів з обліковими даними, навчальні семінари й перевірки внутрішніх і зовнішніх аудиторів. Спеціальні оцінки можуть бути різними за обсягом та періодичністю. COSO наводить обмеження системи внутрішнього контролю, а також роль і обов'язки сторін, що впливають на систему. Обмеження включають помилкову людську думку, неправильне тлумачення інструкцій, помилки, зловживання менеджерів, таємну змову, співвідношення витрат і результатів. COSO визначає недоліки як “умови системи внутрішнього контролю, які заслуговують на увагу”. Звіт про недоліки повинен бути наданий працівнику, відповідальному за розглянуту ділянку, та вищому керівництву.

Вважають, що система внутрішнього контролю є ефективною, якщо всі п'ять наведених компонентів існують та ефективно функціонують щодо операцій, фінансової звітності й виконання встановлених нормативами вимог.

COSO складається з 372 сторінок у двох частинах (друга частина має назву “Інструменти” — *Tools*). Крім того, у 2004 році комітет COSO випустив більш ґрунтовний документ — “Управління ризиками організації. Інтегрований підхід” (*COSO Enterprise risk management — ERM. Integrated Framework*). Документ 1992 року є

складовою частиною документа 2004 року, але одночасно може використовуватися як самостійний документ⁵.

Цікаво, що Закон Сарбейнса-Окслі дозволяє використовувати як концептуальну основу окрім документа COSO також британський нормативний документ — “Керівництво Торнбулла” (*The Turnbull Guidance*, офіційна назва *Internal Control: Guidance for Directors on the Combined Code*) від 1999 року, який складається лише з 41 сторінки! У передмові до видання 2005 року його укладачі зазначають, що британська практика підтвердила справедливність підходу до регулювання, за якого немає потреби детально розписувати методики і процедури внутрішнього корпоративного контролю. “Керівництво Торнбулла” містить подібний до COSO, проте не

Таблиця. Порівняння світових стандартів

Критерій оцінки	COSO (1994)	Turnbull Guidance (2005)	COSO ERM (2004)
Основна цільова група	Керівники підприємства	Керівники підприємства	Керівники підприємства
Внутрішній контроль представляється як	Процес	Процес	Процес
Організаційні цілі внутрішнього контролю	1. Ефективність та економічна доцільність операцій. 2. Надійність фінансового звітування. 3. Узгодженість із відповідними законами та нормативами	1. Ефективність та економічна доцільність операцій. 2. Надійність зовнішнього та внутрішнього звітування. 3. Узгодженість із відповідними законами й нормативами	Управління ризиками підприємства передбачає чотири категорії цілей: 1) стратегічні — цілі високого рівня, пов'язані з місією підприємства; 2) операції — ефективне й доцільне використання його ресурсів; 3) звітування — надійність звітування; 4) відповідність — узгодженість із законами та нормативами
Компоненти або зони	1. Середовище контролю. 2. Оцінка ризику. 3. Контрольні заходи. 4. Інформація та комунікація. 5. Моніторинг	Середовище контролю згадується, але до компонентів не належить. Компоненти: 1) контрольні заходи; 2) процеси інформації та комунікації; 3) процес моніторингу підтримки ефективності системи внутрішнього контролю	1. Внутрішнє середовище. 2. Установлення цілей. 3. Ідентифікація подій. 4. Оцінка ризику. 5. Відповідь на ризики. 6. Контрольні заходи. 7. Інформація та комунікація. 8. Моніторинг
Фокус	Вся організація	Вся організація	Вся організація
Оцінка ефективності внутрішнього контролю	На момент часу	На момент часу	На момент часу
Відповідальність за систему внутрішнього контролю	Керівники підприємства		
Обсяг тексту, сторінок	372	41	Понад 400

⁵ У США незалежні аудитори використовують видання 1994 року — для незалежної оцінки системи внутрішнього корпоративного контролю згідно із Законом Сарбейнса-Окслі документ COSO ERM фактично непридатний, оскільки стосується насамперед внутрішнього, а не зовнішнього контролю.

ідентичний перелік цілей і компонентів внутрішнього контролю (порівняння різних стандартів із внутрішнього контролю див. у таблиці). Вважають, що аналогічний документ Канадського інституту присяжних бухгалтерів (*Canadian Institute of Chartered Accountants*) — “Керівництво з контролю” (*Guidance on Control*, більш відоме як “Критерій контролю” — *Criteria of Control — CoCo*) також є набагато зручнішим для користувачів, ніж COSO⁶.

Аналізуючи світовий досвід нормативного регулювання систем корпоративного фінансового контролю в цілому, доцільно згадати стандарти з внутрішнього контролю, які є складовими збірок стандартів аудиту для проведення незалежного аудиту фінансової звітності, адже сьогодні аудитори зобов’язані перевіряти стан

із корпоративного контролю

CoCo (1995)	SAS 55/78 (1995)	ISA 315 (набирає чинності з 2010)	COBIT (2007)
Керівники підприємства	Зовнішні аудитори	Зовнішні аудитори	Менеджмент, користувачі, аудитори інформаційних систем
Процес	Процес	Процес	Сукупність процесів, включаючи норми, процедури, прийоми й організаційні структури
1. Ефективність та економічна доцільність операцій. 2. Надійність фінансового звітування. 3. Узгодженість із відповідними законами та нормативами	1. Надійність фінансового звітування. 2. Ефективність та економічна доцільність операцій. 3. Узгодженість із відповідними законами та нормативами	1. Надійність фінансового звітування. 2. Ефективність та економічна доцільність операцій. 3. Узгодженість із відповідними законами та нормативами	1. Ефективні й результативні операції. 2. Конфідентність, цілісність і доступність інформації. 3. Надійна фінансова звітність. 4. Узгодженість із відповідними законами та нормативами
1. Мета. 2. Можливості. 3. Здійснення. 4. Моніторинг і навчання	1. Середовище контролю. 2. Оцінка ризику. 3. Контрольні заходи. 4. Інформація та комунікація. 5. Моніторинг	1. Середовище контролю. 2. Оцінка ризику. 3. Контрольні заходи. 4. Інформаційна система. 5. Моніторинг контрольних процедур	1. Планування й організація. 2. Придбання і впровадження. 3. Постачання і підтримка. 4. Моніторинг
Вся організація	Фінансова звітність	Фінансова звітність	Інформаційні технології
На момент часу	За період часу	На момент часу	За період часу
Керівники підприємства			
60	63 (у 2-х документах)	52	187 (у 4-х документах)

⁶ Internal Control Systems // Encyclopedia of Business and Finance. — <http://www.enotes.com/business-finance-encyclopedia/internal-control-systems>.

корпоративного внутрішнього контролю в будь-якому разі, навіть якщо наявність окремого аудиторського висновку з внутрішнього контролю не є обов'язковою (як це вимагають при аудиті публічних компаній у США згідно із Законом Сарбейнса-Окслі). Наприклад, таким є стандарт щодо розгляду структури внутрішнього контролю при аудиті фінансової звітності (*SAS 55*), затверджений Американським інститутом сертифікованих громадських бухгалтерів (*American Institute of Certified Public Accountants*), із внесеними змінами (*SAS 78*). Документи *SAS 55* (1988 рік) і *SAS 78* (1995 рік) надають зовнішнім аудиторам вказівки щодо впливу внутрішнього контролю на планування і проведення аудиторської перевірки фінансової звітності. Останній із документів за основними параметрами повторює COSO, хоча й ставить такий критерій, як надійність фінансової звітності, на перше місце.

Для українських аудиторів з 2004 року (для аудиторів з країн ЄС — з 2005-го) обов'язковими для виконання є Міжнародні стандарти аудиту (*International Standards on Auditing — ISA*). З 2006 року обов'язковим для виконання є *ISA 315* “Визначення та оцінка ризиків суттєвого відхилення шляхом розуміння господарюючого суб'єкта та його середовища” (*Identifying and Assessing Risks of Material Misstatement Through Understanding the Entity and Its Environment*). Аудиторська палата України регулярно видає чинний в Україні переклад Міжнародних стандартів аудиту, який, утім, на один—два роки відстає від оригінального їх тексту. На початку 2008 року вийшли дві нові редакції цих стандартів англійською мовою: одна — поточна, інша набере чинності з 15 грудня 2009 року⁷. У документі *ISA 315* цілі внутрішнього контролю ідентичні відповідним стандартам *SAS 55/78*, а от один із компонентів порівняно з *COSO 1994* та *SAS* дещо модифіковано: компонент “Інформація та комунікація” замінено на компонент “Інформаційна система”.

Цікаво, що з початку 1980-х років Міжнародні стандарти аудиту та додані до них положення про аудиторську практику містили досить детальні вказівки та інструкції щодо оцінки середовища інформаційних систем (наприклад, українські видання 2002 і 2004 років). Так, стандарти 310 “Знання бізнесу”, 400 “Оцінка ризику і внутрішній контроль”, 401 “Аудит у середовищі комп'ютерних інформаційних систем” і Положення про Міжнародну аудиторську практику 1008 “Оцінювання ризиків та внутрішній контроль — характеристики та особливості в КІС” втратили чинність у грудні 2004 року, коли набрали чинності стандарти 315 “Визначення та оцінка ризиків суттєвого відхилення шляхом розуміння господарюючого суб'єкта та його середовища” та 330 “Аудиторські процедури стосовно оцінених ризиків”. На нашу думку, головною причиною цих змін було те, що тепер фактично весь аудит розглядається як комп'ютерний, тобто в умовах застосування бізнесових та обліково-фінансових комп'ютерних інформаційних систем (КІС) і з використанням комп'ютерних методів і засобів аудиту. Саме тому загальні

⁷ Це результат виконання спеціального проекту Міжнародної федерації бухгалтерів із поліпшення змісту та ясності тексту стандартів. У таблиці використано другу, новішу версію цих стандартів.

коментарі та вказівки з цих питань сьогодні містить майже кожний стандарт аудиту. Іншим фактором, який спричинив вилучення детальних вказівок, як зазначає Рада з аудиту Міжнародної федерації бухгалтерів⁸, став такий стрімкий розвиток інформаційних технологій, що згадані положення й стандарти просто застаріли.

На нашу думку, ще однією з причин такого вилучення було те, що останніми роками у світі остаточно оформилася професія аудитора інформаційних систем (*Certified Information Systems Auditor*), з'явилися відповідні професійні організації, такі як Асоціація з аудиту та контролю інформаційних систем (*Information Systems Audit and Control Association — ISACA*), стандарти (*ISACA Standards, COBIT*) та розпочався процес сертифікації фахівців. Так, у 1996 році ISACA вперше випустила документ “Контрольні цілі для інформаційних технологій”⁹ (*Control Objectives for Information and related Technology — COBIT*), завданням яких визначено дослідження, розвиток і поширення сучасних, міжнародних, загальноприйнятих контрольних цілей для інформаційних технологій. COBIT полегшує розуміння інформаційних систем для менеджерів, аудиторів та інших користувачів і пропонує необхідний рівень безпеки й контролю для захисту активів компаній, надає модель для управління інформаційними технологіями. Документ пропонує 34-рівневий процес, який покриває 318 контрольних цілей за чотирма напрямками: планування й організація, придбання і впровадження, постачання й підтримка та моніторинг.

“Контрольні цілі для інформаційних технологій” є корисними і для керівників підприємства, які використовують їх як основу для прийняття рішень щодо інвестицій в інформаційні технології підприємства, і для користувачів інформації та аудиторів. COBIT визначає стратегію розвитку інформаційних систем підприємств, рекомендує необхідне для придбання програмне й технічне забезпечення, що надасть можливість інформаційній системі безперебійно функціонувати в умовах ведення бізнесу. Користувачі інформаційних систем підприємства завдяки COBIT отримують упевненість щодо надійності інформації, а аудитори — можливість легше ідентифікувати контрольні заходи та процедури, здійснювані підприємством, або підтвердити виявлені недоліки в системі корпоративного контролю підприємства.

COBIT класифікує ІТ-ресурси на дані, прикладні системи, технологію, технічні засоби та людей. Дані визначаються в їх найширшому розумінні та включають не лише цифри, текст і дати, а й інші об'єкти — графічні дані та звуки. Під прикладними системами розуміють сукупність ручних і автоматичних процедур. Технологія включає апаратні засоби, операційні системи, мережеве устаткування тощо, технічні засоби — ресурси, використовувані для розміщення й підтримки інформаційних систем. Під ресурсом “люди” слід розуміти індивідуальні

⁸ Mancino J. Proposal to Withdraw IT-Related IAPs // IAASB Main Agenda. — December 2004. — P. 2004–2039. — <http://www.ifac.org/IAASB/Meeting-FileDL.php?FID=0915>.

⁹ Поточну версію COBIT 4.1 датовано 2007 роком.

навички і здібності планувати, організовувати, придбавати, доставляти, підтримувати та контролювати інформаційні системи й послуги.

Структура COBIT передбачає найважливіші правила для конкретних ІТ-процесів. Схема документа визначає бізнес-задачу, що досягається з допомогою правил контролю, і ІТ-ресурси, керовані процесами; формулює можливі засоби контролю та список найважливіших цілей контролю щодо конкретного випадку.

Порівняємо деякі аспекти розглянутих стандартів. COBIT, COSO, Turnbull Guidance, SAS 55/78 та ISA 315 містять багато спільних концепцій контролю. Фактично, більш пізні документи побудовано на концепціях, розроблених у більш ранніх документах. Проте, оскільки розглянуті нормативні документи розробляли різні органи для різних цільових груп, можливі деякі невідповідності між документами. Водночас кожен із них фокусується на внутрішньому контролі й конкретній цільовій групі (наприклад, ІТ-фахівці, менеджмент, зовнішні аудитори), приділяє значну увагу створенню й оцінці засобів контролю.

Згадані документи надають визначення внутрішнього контролю, описують його компоненти і передбачають інструменти його оцінки. COBIT додатково пропонує всебічний аналіз реалізації моделі й обговорення питань внутрішнього контролю, пов'язаних з інформаційними технологіями.

Усі документи визначають менеджмент (керівництво підприємства) відповідальним за забезпечення належного функціонування засобів контролю. COBIT передбачає відповідальність менеджменту в моніторингу всіх процесів інформаційної технології. Оскільки засоби контролю призначено для функціонування протягом тривалого часу, то COSO визначає обов'язки менеджменту щодо спостереження за всією системою внутрішнього контролю щодо всіх поточних видів діяльності, вбудованих в систему контролю, і за всіма спеціальними оцінками, орієнтованими на спеціальні види діяльності й сфери.

Визначаючи поняття “внутрішній контроль”, документи передбачають, що компанія встановила цілі для своїх операцій. COBIT визначає, що ці цілі підтримуються бізнес-процесами, які, у свою чергу, підтримуються інформацією, наданою з допомогою використання інформаційної технології. Бізнес-вимоги для цієї інформації задовольняються через адекватні контрольні заходи. COSO класифікує цілі на операційні, цілі фінансової звітності та відповідність нормативам. Тоді як COSO розглядає цілі у всіх трьох категоріях, SAS 55/78 та ISA 315 концентрують увагу переважно на цілях щодо фінансової звітності. Документ COBIT сфокусовано винятково на засобах контролю інформаційної технології, яка підтримує цілі бізнесу. COSO надає широке охоплення щодо організації в цілому, а SAS 55/78 та ISA 315 фокусуються на аудиті фінансової звітності. COSO і Turnbull Guidance є самодостатніми документами, SAS 55/78 та ISA 315 — частиною аудиторських стандартів.

COBIT, COSO, SAS 55/78 та ISA 315 різняться також підходом і глибиною розгляду інформаційних систем. Головне призначення COBIT — створення системи, яка поєднує безпеку й контроль в інформаційних технологіях. Документ установлює

чіткий зв'язок між засобами контролю інформаційних систем і бізнес-цілями. Додатково передбачаються загально визнані цілі контролю для кожного процесу інформаційної технології, що дає можливість надавати практичні рекомендації щодо контролю для всіх зацікавлених сторін. Документ також надає засоби для здійснення взаємодії між керівниками підприємств, користувачами фінансової інформації та аудитором щодо засобів контролю інформаційних систем.

COSO забезпечує інструментами, які може бути використано для оцінки системи внутрішнього контролю. Другий том документа присвячено методикам і питанням, що використовуються для перевірки засобів контролю. Водночас SAS 55/78, ISA 315 і Turnbull Guidance не надають конкретних форм чи інструментів для оцінки системи контролю.

Отже, для українського бізнес-середовища ситуація складається таким чином: хоча зовнішні аудитори, які перевіряють показники фінансової звітності, мають загальні вказівки щодо оцінки ризиків стосовно корпоративних систем контролю (*ISA 315*), будь-які детальні чинні нормативні акти, які слугували б методичною основою для побудови й оцінки корпоративних систем внутрішнього контролю, практично відсутні.

На нашу думку, розвиток консалтингового ринку й ринку інформаційних технологій, поліпшення загальної економічної ситуації та зростання конкуренції безперечно приведуть до адаптації світових нормативних актів у галузі корпоративного фінансового контролю в Україні.

Це можливо шляхом:

- створення національних нормативів контролю на основі міжнародних;
- адаптації існуючих у світі нормативів.

Обидва шляхи можуть виявитися ефективними. Однак, на нашу думку, адаптація такого документа, як COSO, є недоцільною. Як ми переконалися, міжнародні стандарти аудиту вже містять основні положення з питань корпоративного внутрішнього контролю. Адаптувати ж детальне та чимале за обсягом керівництво з методик внутрішнього контролю, орієнтоване на документообіг та законодавство США, недоречно. Можливо, ефективніше буде закріпити загальні вимоги до корпоративних систем внутрішнього контролю на законодавчому рівні, наприклад як частину Закону України “Про акціонерні товариства”, використавши положення документів Turnbull Guidance, ISA 315 та COSO ERM.

З інформаційними технологіями ситуація інша. Технологічний процес обробки обліково-фінансової інформації на підприємстві мусить бути інтегрованим незалежно від того, в яких країнах працює компанія. COBIT, являючи собою системний документ, передбачає визначення засобів контролю і цілей контролю для специфічних процесів інформаційної технології та використовується насамперед ІТ-фахівцями на підприємстві та зовнішніми консультантами з автоматизованих систем. На нашу думку, найефективнішим буде повна адаптація цього нормативного документа в Україні.