УДК 657

СИСТЕМА ВНУТРЕННЕГО КОНТРОЛЯ И КОНТРОЛЬ В ИНФОРМАЦИОННОЙ СИСТЕМЕ БУХГАЛТЕРСКОГО УЧЕТА[1]

Катерина ШЫМЧЫК-МАДЕЙ
к.е.н., доцент кафедры бухгалтерского учета,
Краковский Экономический Университет
e-mail: szymczyk@uek.krakow.pl

Ян МАДЕЙ
к.е.н., доцент кафедры информатики,
Краковский Экономический Университет
e-mail: jan.madej@uek.krakow.pl

Анотація. Кожне підприємство має систему бухгалтерського обліку. Її правильне функціонування є як формальною вимогою законодавства, так і необхідною умовою ефективної господарської діяльності. Однак часто тяжко отримати відповідь на питання чи правильно функціонує система бухгалтерського обліку без проведення відповідного внутрішнього контролю. Існуючі загальні процедури контролю, що стосуються інформаційних систем, не завжди можуть застосовуватися в інформаційній системі бухгалтерського обліку. Дана стаття є пропозицією поділу процедур контролю в інформаційній системі бухгалтерського обліку на загальний контроль і контроль додатків.

Аннотация. Каждое предприятие имеет систему бухгалтерского учёта. Ее правильное функционирования является как формальным требованием законодательства, так и необходимым условием эффективной хозяйственной деятельности. Однако получение ответа на вопрос правильно ли функционирует система бухгалтерского учёта, часто бывает затруднительным без проведения соответствующего внутреннего контроля. Существующие общие процедуры контроля, касающиеся информационных систем, не всегда могут применяться в информационной системе бухгалтерского учёта. Данная статья является предложением разделения процедур контроля в информационной системе бухгалтерского учёта на общий контроль и контроль приложений.

Ключові слова: *внутрішній контроль, контроль додатків, інформаційна система бухгалтерського обліку.*
Ключевые слова: *внутренний контроль, контроль приложений, информационная система бухгалтерского учёта.*

Постановка проблемы. Понятие контроля имеет много значений. В основном контроль определяется как процесс оценки, то есть, сравнение фактического состояния с требуемым или плановым состоянии, которые определяются, например, нормами права, финансовыми нормативами, планами, решениями руководства и т.д. Определение внутреннего контроля, основанного на данных предположениях, предложил Е. Теребуха [22]. Он определил внутренний контроль как „действия, проводимые в границах функции управления руководством предприятия, а также назначенными для этого ячейками и людьми. Эти действия предусматривают проверку – в основном с помощью сравнения с поставленными заданиями, выданными внутренними распоряжениями и действующим законодательством – легальности, точности и правильности проведённых на предприятии хозяйственных операций, как потенциальных, так и фактически проведённых, с целью повышения эффективности деятельности, гарантирования защиты общественного имения, а также выполнения обязывающих норм права и внутренних инструкций".

Однако в настоящее время все чаще отходится от функционального понимания внутреннего

[1] Publikacja została sfinansowana ze środków przyznanych Wydziałowi Zarządzania Uniwersytetu Ekonomicznego w Krakowie w ramach dotacji na utrzymanie potencjału badawczego.

контроля. Его представляют в систематическом понимании, говоря о „системе внутреннего контроля" (СВК), как системе, охватывающей поведение управляющих, методы, процедуры и другие инструменты, которые могут гарантировать рациональную уверенность, что цели хозяйственного субъекта будут достигнуты [9; 19; 21]. Однако и дальше традиционно за основной вид внутреннего контроля, который проводится в системе бухгалтерского учёта, считается учётно-финансовый контроль. В то же время практически на каждом предприятии бухгалтерский учёт ведётся с помощью информационных технологий и система бухгалтерского учёта по сути стала „информационной системой бухгалтерского учёта" (ИСБО). Поэтому проведение на предприятии только учётно-финансового контроля не гарантирует получение точного образа и обнаружение всех ошибок. Необходимым является расширение набора элементов контроля контролем, непосредственно касающимся информационной среды, в которой ведётся бухгалтерский учёт.

Целью данной **статьи** является обращение внимание на необходимость расширения системы внутреннего контроля (в сфере информационной системы бухгалтерского учёта) за счет других видов контроля, таких, например, как общий контроль и контроль приложений. В статье представлена краткая характеристика данных видов контроля и показана взаимозависимость между ними и элементами системы внутреннего контроля.

Системный подход к проблематике внутреннего контроля мы можем чётко увидеть в западных стандартах. Уже в 90-х годах XX века Международная Организация Высших Органов Контроля INTOSAI [18] отметила, что „внутренний контроль является инструментом управления, который используется для получения рациональной уверенности в том, что цели управления были достигнуты. В свою очередь система внутреннего контроля это целая система контрольных финансовых и других решений вместе с организационной структурой, методами, процедурами и службами внутреннего контроля, который установлен руководством и помогает ему в экономном, продуктивном и эффективном ведении интересов контролируемого субъекта; гарантирующий выполнение политики руководства".

Подобным образом данная проблематика была представлена и в других нормах и стандартах, разработанных организациями, имеющими влияние на развитие внутреннего контроля и аудита (например, в *Рапорте Cadbury* [1], *Критериях контроля Канадского Института Дипломированных Бухгалтеров* [4], *Стандартах внутреннего контроля Европейской Комиссии* [8], или в *Интегрированной концепции внутреннего контроля* [7].

В соответствии с вышеприведенными документами необходимо принять, что *система внутреннего контроля является системой, включающей в себя все элементы организации (средства, процессы, структуру, культуру), которые помогают в достижении поставленных данной организацией целей и гарантируют (на соответствующей уровне) эффективную и производственную деятельность, правильность финансовых процессов, соответствие с законодательством.* Это означает, что внутренний контроль охватывает всю организацию, а его действия встроены в среду, процедуры и задания всех членов организации, которые реализуют их в соответствии с занимаемой должностью.

Система внутреннего контроля состоит из соответствующим образом взаимосвязанных и взаимодополняющих элементов. Именно сумма данных элементов позволяет эффективно и качественно достигать поставленные цели. В большинстве рекомендаций и стандартов, связанных с внутренним контролем, наводится пять ключевых элементов системы внутреннего контроля (СВК), а именно [7; 9; 11; 14; 17; 19; 21]:

- среда внутреннего контроля;
- управление риском;
- механизмы внутреннего контроля;
- информирование и передача данных;
- мониторинг и исправление ошибок.

Среда контроля это деятельность руководства, формирующая уровень значения внутреннего контроля и гарантирующая необходимые условия для достижения основных целей контроля. Она включает стиль управления, организационную культуру и ценности, признаваемые ее работниками, а также определяет границы, в которых работают другие элементы контроля.

Среда внутреннего контроля включает прежде всего управление человеческими ресурсами (через соответствующую кадровую политику и развитие квалификаций работников) и решения в сфере организации (включающие философию и стиль деятельности руководства, организационную структуру, гарантирующую соответствующие взаимодействия между СВК и другими системами предприятия, наделение правами и

ответственностью).

Управление риском в контексте СВК это процесс, который может быть по разному формализован, но всегда в нем можно выделить следующие этапы:

– идентификация объектов, риск которых будет анализироваться – то есть информационных, финансовых, человеческих, материальных и нематериальных средств (например, хорошая репутация, доверие клиентов);

– идентификация угроз, склонности и результатов появления угроз;

– оценка риска – то есть определение вероятности появления угроз;

– определение уровня *допустимого риска* и *остаточного риска*[2]

– определение требований в сфере контроля – то есть определение, что и каким образом должно контролироваться;

– определение возможности и эффективности управления риском – то есть анализ возможности ограничения угроз и их последствий в ходе внедрения механизмов контроля и сравнение затрат механизмов контроля с преимуществами их внедрения;

– выбор и внедрение механизмов контроля.

Механизмы внутреннего контроля это контрольные операции, которые проводятся на основе разработанных процедур. К наиболее важным механизмам контроля можно отнести [5; 12; 15; 23]:

– осмотры – то есть требуемые руководством отчеты, позволяющие оценить прогресс в реализации поставленных целей;

– надзор – его целью является убеждение, что задания, выплывающие с принятой системы контроля, реализуются;

– контроль доступа к средствам – его целью является ограничение доступа к средствам (например, финансовым, материальным, информационным) неуполномоченным лицам;

– инвентаризация – это одно с основных действий внутреннего контроля, которое позволяет сравнить отображенные в учетных книгах данные с их фактическим состоянием, а также позволяет урегулировать найденные несоответствия с лицами, ответственными за вверенное им имущество;

– соблюдение лимитов – то есть контроль установленных для некоторых действий лимитов (в особенности финансового характера) и анализ случаев их несоблюдения;

– одобрения и авторизации – то есть одобрение уполномоченным работником всех хозяйственных операций перед их реализацией, а также выполнение связанных с данными операциями действий только уполномоченными работниками;

– разделение обязанностей – применяется с целью уменьшения или обнаружения: риска ошибки, расточительности или неправильных действий;

– документирование системы внутреннего контроля – то есть точное документирование процедур, инструкций, указаний руководства, обязанностей, используемых в СВК;

– документирование и регистрация всех хозяйственных операций;

– регистрация отступлений – то есть документирование и представление для подтверждения уполномоченному лицу каждого отступления от установленных процедур, инструкций или распоряжений;

– процедуры, гарантирующие непрерывную деятельность – разработка руководством соответствующих механизмов позволяющих сохранить непрерывность операции в каждом моменте и в каждых условиях (например, в случае изменения информационной системы, отсутствия работника);

– проверка соответствия учетных записей с состоянием средств и обязательств;

– другие механизмы и приемы контроля, как, например, движение на должностях, которые в особенности наражены на ошибки, контроль бланков (например, использование подотчетных бланков, проверка хронологии (порядка) формуляров, ограничение доступа к формулярам).

Информирование и передача данных является основой правильного функционирования системы внутреннего контроля. Однако передаваемая информация должна быть [7; 9; 14; 19; 21]:

– целенаправленной – практична в решении определенных проблем, связанных с принятием решения;

– правдивой – соответствующая описываемой реальности;

– актуальной – приспосабливающая время обработки информации к длине цикла принятия

[2] Риск, который осознанно никаким образом не ограничивается, поскольку был принят – называется допустимым риском. Это риск, который не угрожает реализации поставленных заданий, а дальнейшее его снижение является неэкономным. Остаточный риск это риск, который остается после внедрения механизмов контроля. На практике такой риск существует всегда, поскольку ни один ресурс не является абсолютно безопасным. Важно, однако, чтобы руководство было осведомлено о существовании остаточного риска и принимало его.

решения, который она обслуживает,

– полной – содержащая все данные, необходимые принимающим решения;

– всесторонней – учитывающая сложность и многогранность каждой потенциальной ситуации, связанной с принятием решения, а также содержащая данные с различных сфер и разных точек зрения;

– в меру подробная – „не слишком подробная, и не слишком общая",

– связана с обоснованными финансовыми затратами – то есть, полученный в результате использования информации эффект должен хотя бы сравнятся с понесенными на получение данной информации затратами.

Мониторинг системы внутреннего контроля выплывает из факта, что создание системы внутреннего контроля не является одноразовым актом, но процессом, в котором руководство оценивает эффективность принятой системы и указывает на необходимые направления её модификации. Целью мониторинга является удостоверение в том, что выплывающие с принятой системы внутреннего контроля и задания реализуются, а качество системы не ухудшается со временем. Более того, мониторинг позволяет не только эластично реагировать на меняющиеся условия, но также часто позволяет решать поточные проблемы. В практике на предприятиях применяется:

– операционный мониторинг – используется в обычной операционной деятельности. Предусматривает управленческие и наблюдательные действия, а также другие действия, Которые реализуются работниками в ходе выполнения своих обязанностей;

– периодический мониторинг – проводится тогда, когда операционный мониторинг является недостаточным для проведения объективной оценки функционирования системы внутреннего контроля и обязательным является предоставление руководству независимой точки зрения виде отдельной оценки по поводу функционирования системы внутреннего контроля.

Проблематика внутреннего контроля в информационной среде, в которой действует Информационная система бухгалтерского учёта, была поднята во многих публикациях [2; 5; 6; 10; 13; 20]. Все автора сходятся во мнении, что если бухгалтерский учёт действует в информационной среде, то связи со специфическими чертами данной среды и возникновение большего количества разнообразных угроз, система внутреннего контроля должна быть более расширена.

Однако часто в публикациях отсутствует подробный ответ на вопрос, что должно входить в перечень этих дополнительных методов контроля и как они должны проводиться. проведённые библиографические исследования, в особенности анализ международных решений, позволяют сделать следующие выводы. В соответствии с рекомендациями международных стандартов, которые касаются исследования информационной среды (3; 13; 16), кроме учётно-финансового контроля в информационной системе бухгалтерского учёта, необходимо дополнительно проводить:

– *общий контроль (general controls)* – проводится для всей информационной среды, в том числе для информационной системы бухгалтерского учёта;

– *контроль приложений (application controls)* – проводится для программного обеспечения, которое используется в информационной системе.

Общий контроль и контроль приложение взаимосвязаны между собой. Общий контроль прежде всего необходим для обеспечения правильного функционирования целое информационной системы, поэтому он непосредственно влияет на эффективность контроля приложений. В особенности это означает, что если общий контроль проводится неправильно, то также нельзя доверять и контролю приложений. Это выплывает с того, что неправильный общий контроль перечеркивает достоверность даже сильного контроля приложений.

По отношению к представленным выше элементам системы внутреннего контроля – „общий контроль" должен быть включён в „среду контроля", а „контроль приложение" должен проводиться в границах „механизмов внутреннего контроля". Зависимость между данными элементами системы внутреннего контроля а и информационным контролем представлена на рис. 1.

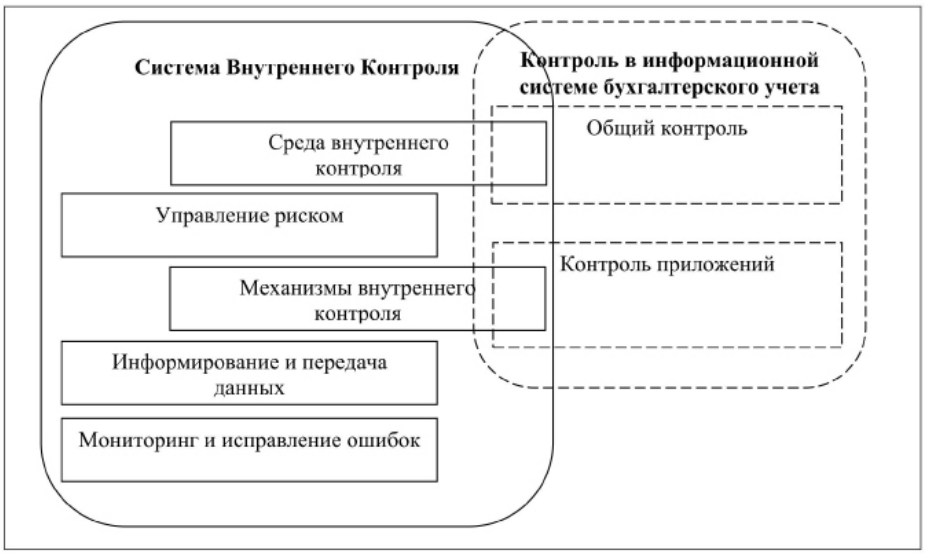

Рис. 1. Система внутреннего контроля и контроль в Информационной системе бухгалтерского учета

Источник: собственная разработка авторов

Целью общего контроля является гарантирование правильного функционирования и развития всей информационной среды [16]. Поэтому к общему контролю относятся все действия (например, организация труда, сохранение пользователей, указанию руководства, подготовка пользователей, процедуры действий, покупка оборудования и программного обеспечения, сохранение ресурсов и т.д.), которые предусматривают сохранение правильного функционирования информационной системы на предприятии.

Принимая во внимание цель общего контроля, к ним можно отнести такие действия, как:

1) организация процесса обработки, а именно:

– разработка соответствующей организационной структуры отдела информатики;

– определение участия отдельных организационных единиц предприятия в процессе обработки данных;

– соответствующее разделение заданий между участниками обработки данных в ходе правильного определения их полномочий, обязанностей и ответственности;

– определение руководство соответствующих ресурсов наблюдения за функционированием отдела информатике и процесса обработки данных;

– определение хода действий и графика процесса обработки;

2) эксплуатация и использование средств системы, а именно:

– соблюдение процедур и принципов процесса обработки;

– контроль доступа к средствам системы;

– правильное использование программного обеспечения и компьютерного оборудования;

– управление носителями данных;

3) гарантия непрерывности и безопасности процесса обработки, а именно:

– соблюдение пользователями общих принципов безопасности;

– сохранение ресурсов системы от не уполномоченного доступа;

– создание и хранение копии данных и программного обеспечения;

– разработка и соблюдение охранных и аварийных процедур;

– организация обучения пользователей в сфере обслуживания программ и оборудования, а также обучение в сфере охраны и безопасности системы;

– сохранение ресурсов (например, оборудования, программного обеспечения, данных) от результатов появившихся угроз;

4) поддержание и развитие информационной системы, а именно:

– уход за правильным функционирование программ и компьютерного оборудования;

– анализ нужд в сфере развития информационной системы (например, покупка нового программного обеспечения, оборудования, технологий обработки данных);

– обеспечение соответствующего качества компьютерного оборудования и инфраструктуры;

– контроль эффективности информационной системы;

– разработка и реализация плана осмотров, консервирования и чистки компьютерного оборудования;

– разработка и реализация плана и методов развития информационной системы;

5) разработка полной документации информационной системы, её хранение в безопасном месте и открытия доступа пользователям к той части документации, которая нужна им во время выполнения работы.

На предприятии должны быть выделены информационные службы для проведения общего контроля. Если это возможно и не затратно, должен быть также назначен специалист по делам безопасности информационной системе.

Целью контроля приложений является прежде всего гарантия достоверности используемого программного обеспечения в ходе получения уверенности, что полученные с их помощью данные и информация являются правильными, то есть, что на этапе ввода, передачи, хранения и получения данных не появляются ошибки. Контроль приложений должен включать:

– ввод данных (контроль входящих данных);

– обработку данных (контроль обрабатываемые данных);

– получение результатов (контроль выходящих данных).

Контроль входящих данных должен проводиться уже во время ввода данных и охватывает такие виды контрольных действий, как [6]:

– контроль сумм – проверка, соответствует ли суммы с вводимых документов суммам, Полученным с другого источника (например, при ведение счетов фактур их суммы должны соответствовать сумам, поданным контрагентами, например, в документе перевоза);

– контроль количества – проверка, соответствует ли количество введённых в систему единиц из документа количеству единиц, полученному с другого источника;

– контроль количества документов – проверка соответствует ли количество введённых в систему документов количество документов, полученному из другого источника (например, поданная контрагентом);

– контроль общих сумма – проверка соответствует ли сумма всех полей (например, сумма всех товаров) общей сумме;

– контроль порядка – проверка является ли нумерация документов непрерывной;

– контроль повторений – проверка, не были ли документы введены несколько раз;

– контроль лимитов – проверка, не превышает ли введённая с ума определённого лимита (например, не был ли превышен для данного клиента определённый лимит на допустимую величину покупки в торговый кредит);

– контроль диапазона – проверка, соответствует ли данные установленному диапазону;

– контроль длины – проверка, вместились ли текстовые данные в установленный диапазон;

– контроль правильности данных – проверка, соответствует ли введённые данные установленным критериям;

– контроль рациональности – определение, имеют ли смысл введённые данные;

– словарный контроль – проверка, происходит ли введённые данные с определённого словаря данных;

– проверка контрольных цифр – проверка, соответствует ли вычисленная контрольная цифра поданной цифре;

– контроль полноты – проверка, все ли требуемые поля заполненный данными;

– контроль логических связей – проверка имеют ли смысл введённые данные вместе с данными, которые были уже введены или приняты косвенно (например, дата выставления счета фактуры не должна быть позже чем дата её отображение в бухгалтерском учёте);

– контроль правильности цифровой подписи – проверка, является ли цифровая подпись данных правдивой.

Если во время контроля вводимое данных будут прикрыты ошибки, то в зависимости от способа ведения данных нужно откинуть всю партию вводимых данных, задержать введение данных, пока не будут выправлены ошибки или отклонение ошибочных данных и дальнейшее введение правильных данных.

Контроль обрабатываемых данных предусматривает предотвращение несанкционированного изменения или удаления данных. Во время обработки данных применяются следующие виды контроля:

– контроль „второй руки” – Подтверждение начало обработки другим лицом;

– повторное авторизации – дополнительная проверка пользователя перед началом обработки (например, введение дополнительного пароля

перед перечислением денег);

– ручные пересчеты – ручная проверка некоторых данных (например, во время выплаты наличных в кассе кассир вручную пересчитывает выплачиваемую сумму).

Контроль выходящих данных это контроль, целью которого является проверка, Имеют ли к данным доступ исключительно уполномоченные лица в определённые сроки и определённых местах. Поэтому нужно обратить внимание на следующие проблемы:

– доступ к выходящим данным – проверка, имеют ли доступ к этим данным только уполномоченные пользователи;

– регистрация случаев доступа к выходящим данным, то есть, какие данные, кому, когда, кем и на какой основе были поданы.

Дополнительно нужно контролировать и ограничивать возможность получения данных с приложений без генерирования выходящих данных с помощью соответствующего модуля.

Выводы. В завершение нужно отметить, что хотя постулат расширение сферы внутреннего контроля в информационной системы бухгалтерского учёта на общий контроль и контроль приложений кажется относительно простым в выполнении, то на практике стоит ожидать ряда связанных с ним проблем. Проблематика общего контроля и контроля приложений не является широко известной в среде ответственных лиц за проведение внутреннего контроля в информационной системе бухгалтерского учёта предприятия. Также отсутствуют соответствующие процедуры и рекомендации, на основе которых данный контроль проводился бы в системе бухгалтерского учёта. Существующие общие процедуры, касающиеся информационных систем, не всегда могут применяться в информационной системе бухгалтерского учёта. Не хватает также стандартизированной формы презентации и способа сравнения полученных во время такого контроля результатов. Поэтому, как сферу дальнейших исследований можно предложить попытку разработки соответствующих процедур проведения общего контроля и контроля приложений в информационной системе бухгалтерского учёта.

Список використаних джерел

1. Cadbury Report, Report of the Committee on the Financial Aspects of Corporate Governance, Gee and Co Ltd., Londyn December 1992.

2. Ciesielczyk T., Watras G., Kontrola wewnętrzna w środowisku informatycznym, Prace Naukowe Akademii Ekonomicznej we Wrocławiu nr 872, Wrocław 2000.

3. COBIT 5th Edition, IT Governance Institute, 2012.

4. Criteria of Control, Canadian Institute of Chartered Accountants, Toronto 1995.

5. Czerwiński K., Audyt wewnętrzny, Wyd. InfoAudit Sp. z o.o., Warszawa 2004.

6. Forystek M., Audyt informatyczny, Wydawnictwo InfoAudit Sp. z o.o., Warszawa 2005.

7. Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, Jersey City 1992.

8. Internal Control, European Commission – Budget Directorate-General, http://europa.eu.int/comm/budget/ic/index_en.htm.

9. International Professional Practices Framework (IPPF), The Institute of Internal Auditors, Wydawnictwo The IIA Research Foundation, 2013.

10. Knedler K., Stasik M., Audyt wewnętrzny w praktyce, Wydawnictwo Audit Solutions i Akademia Kształcenia Kadr, Warszawa 2014.

11. Kontrola Wewnętrzna. Poradnik dla Członków Zarządów na temat Jednolitego Kodeksu, Polski Instytut Kontroli Wewnętrznej, Warszawa 1999.

12. Kuc B.R., Audyt wewnętrzny, teoria i praktyka, Wyd. Menedżerskie PTM, Warszawa 2002.

13. Praktyczne zasady zabezpieczania informacji, Norma PN-ISO/IEC 27002:2014-12, Wydawnictwo Polski Komitet Normalizacyjny.

14. Rekomendacja H – dotycząca kontroli wewnętrznej w banku, Generalny Inspektorat Nadzoru Bankowego NBP, Warszawa 2002.

15. Rola Z., Kontrola wewnętrzna, kontrola finansowa i audyt w jednostkach sektora finansów publicznych, Wyd. ALPHA pro Sp. z o.o., Ostrołęka 2013.

16. Słownik terminologii związanej z kontrolą i audytem systemów informatycznych, The Information Systems Audit and Control Association, (w:) http://www.isaca.org.

17. Standards for Internal Control in the Federal Government, General Accounting Office of USA, November 1999.

18. Standards for the Professional Practice of Internal Auditing, The International Organization of Supreme Audit Institutions, 1992.

19. Standardy kontroli finansowej w jednostkach sektora finansów publicznych, Komunikat Nr 1 Ministra Finansów z dnia 30 Stycznia 2003 r. , Dz. Urz. Ministra Finansów z 2003 r., Nr 3, poz. 13, Biuletyn Skarbowy Ministerstwa Finansów 1/2003.

20. Stępniewski J., Audyt i diagnostyka firmy, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław 2001.

21. Struktura systemów kontroli wewnętrznej w instytucjach bankowych (Framework of Internal Control Systems in Banking Organisations), Komitet Bazylejski ds. Nadzoru Bankowego, 1998, tłumaczenie Generalny Inspektorat Nadzoru Bankowego NBP.

22. Terebucha E., Zasady wewnętrznej kontroli finansowo-księgowej w przedsiębiorstwach transportowych, Wyd. Komunikacji i Łączności, Warszawa 1965.

23. Winiarska K., Kontrola wewnętrzna w jednostkach gospodarczych, Polskie Wydawnictwo Ekonomiczne, Warszawa 2010.