doi: 10.2478/v10313-012-0014-7
2012 /15

Assessing the Need of Information Technology Control Environment Establishment

Ruta Pirta[1], Renate Strazdina[2], [1-2]*Riga Technical University*

***Abstract* – IT controls as part of organization internal control system are an important mechanism for ensuring that the business objectives are met. However, empirical observations show that organizations frequently do not establish an appropriate IT control environment. In this research paper, results of IT general controls (ITGC) audits are analysed at 61 Latvian companies with the purpose of assessing the need for establishing an IT control environment. Research results provide evidence that organizations with an effective IT control environment have fewer identified significant deficiencies in ITGC audits; there are fewer IT-related risks and the potential impact and probability of the identified risks is lower. These observations suggest that the IT control environment helps organizations achieve better quality indicators and reduce IT-related risks.**

***Keywords* – IT audit, IT controls, IT control environment, ITAC, ITGC**

I. Introduction

These days, most essential tasks in the financial reporting processes are performed and supported by utilizing information technology (IT). In order to ensure reliable financial reporting, more and more companies emphasize the use and development of effective IT controls in this dynamic environment [1]. The role of IT controls and audit has become a critical mechanism for ensuring the integrity of information systems (IS) and the reporting of organization finances [2].

However, empirical observations show that Latvian organizations frequently do not establish an appropriate IT control environment. The main aims of this research paper are as follows: 1) to assess the need for and efficiency of the IT control environment in Latvian companies; and 2) to evaluate the impact of the IT control environment on organizations' performance in those core business areas that are dependent on or closely related to IT.

In this research paper, ITGC audits will be viewed only as part of annual financial audits.

II. IT Controls, IT Control Environment and IT Controls Audit

IT controls are specific activities performed by persons or systems designed to ensure that information systems operate continuously and properly.

IT control objectives relate to the confidentiality, integrity, and availability of data and the overall management of the IT function of the business enterprise [3].

IT controls are frequently categorized into IT general controls (ITGC) and IT application controls (ITAC). ITGC include security management, software acquisition, development and maintenance that can support reliable application controls and ensure the continued operation of information systems [4]. ITAC are those controls that pertain to the scope of individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting [5].

The IT control environment is an interrelated set of IT controls that are applied to an integrated IT environment. IT controls are defined and described in several international standards and methodologies like COBIT, ITIL and ISO 27001, 27002 and others.

IT controls audit is an audit that evaluates the organization's IT-related controls (including their design and operation). IT controls audit might be held as part of an IT audit or as part of a financial/operational audit. Both ITGC and ITAC may be audited during the IT controls audit, in accordance with the scope of the specific audit.

III. Research Design

In this research, the results of ITGC audits are analysed at 61 Latvian companies, operating in the following industries – insurance, technology, energy, transport & logistics, industrial production, real estate, wholesale, retail, service, finance and pharmacy (see Fig. 1). Firstly, the results are summarized to show the overall situation in Latvian companies; secondly, the results are analyzed to see the difference between organizations with an established IT control environment and organizations without it.

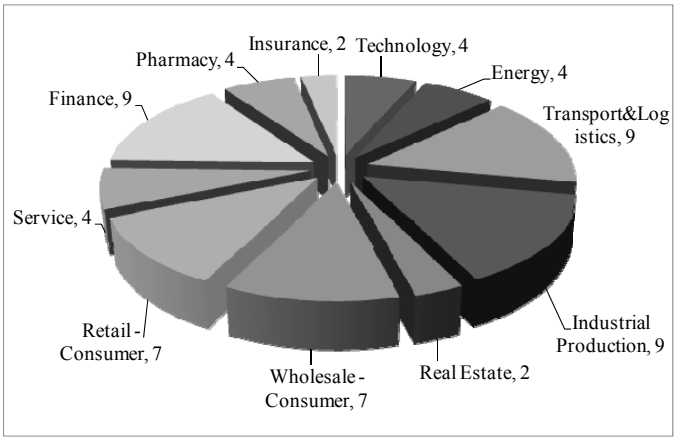

Fig. 1. Industries of audited organizations

The ITGC audits have been held as part of the annual financial audit in order to get confidence that information processed by organization's information systems (IS) is

reliable. The following steps have been performed during the ITGC audits: (1) understanding of the organizations' IT environment (including the IT controls applied); (2) understanding and evaluation of internal control components related to IT; and (3) understanding, evaluation and testing of relevant ITGCs (scoping of relevant ITGC work; evaluation of design of relevant ITGCs; testing of relevant ITGCs; evaluation of results of ITGC testing). Figure 2 shows the performed financial audit/ITGC audit steps and their relation to the requirements of the International Standard of Auditing (ISA) 315.

Notations used in Fig. 2:

ISA 315 requrement - ISA 315 requirement

Audit step - Financial audit/ITGC audit step related to ISA 315 requirement

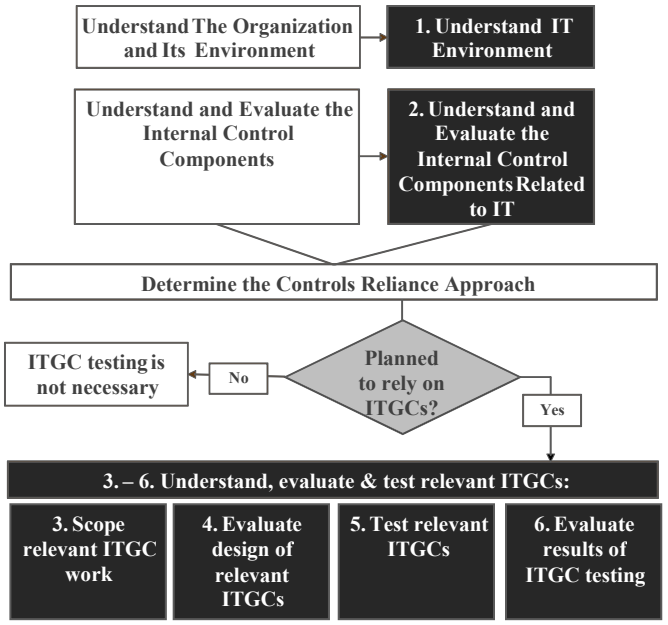

Fig. 2. Financial audit/ITGC audit steps and ISA 315 requirements

To understand the IT related controls in organizations, the following areas have been reviewed – (1) IT governance (control objective – to ensure that IT processes are designed and maintained according to the organization's strategy and regulating rules), (2) program development (control objective - to ensure that systems are developed, configured, and implemented to ensure integrity of the financial reporting process)/program changes (control objective - to ensure that changes to application programs are authorized, performed, tested and implemented in a manner that maintains the integrity of the application), (3) computer operations (control objective - to ensure that production systems are processed completely and accurately and that processing problems are identified and resolved completely and accurately to maintain the integrity of financial data); and (4) access to programs and data (control objective - to ensure that access granted to in-scope programs and data, upon authentication of the user's identity, is both authorized and aligned with job responsibilities).

IV. Research Results

Research results show that in 3 years 95% of audited companies have identified deficiencies in access rights management area, 92% – in computer operations area, 33% – in program development/program change area and 31% – in IT governance area. Figure 3 shows a number of companies with issues found in IT control areas.

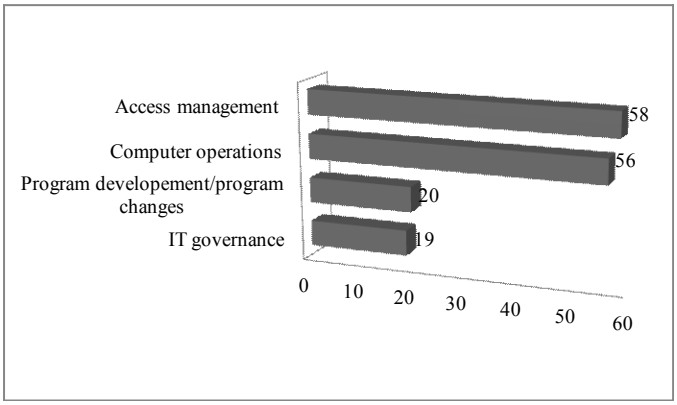

Fig. 3. Companies with issues in IT control areas

Table I shows the frequently identified deficiencies in all audited areas (IT governance, program development/program changes, computer operations, access to programs and data) and their risk level (risk that may arise because of identified deficiency). The risk level has been determined using the expert assessment method.

TABLE I

Frequently Identified Deficiencies

Access to programs and data		
Low risk	**Medium risk**	**High risk**
-	Server room is not appropriately equipped. Passwords (IS, network) security settings are too weak. IS access rights are not divided in separate groups according to access level. Internal wireless network is encrypted with comparatively weak encryption protocol. Owners of IS are not formally assigned. Administration procedure of formal	IS are not secured with passwords.

	user access rights does not exist. There are unused/unclosed user accounts. Granted access rights have not been frequently reviewed by information systems owners. One user account is used by several persons. IS developers have full access to IS production environment.	
Program development/program changes		
Low risk	**Medium risk**	**High risk**
Formal testing procedure does not exist. Formal change request procedure does not exist.	Changes made are not documented. It is not possible to trace who has made changes. IS source code is kept in an inappropriate place.	Changes are not tested prior to implementation. Changes are implemented without formal IS owner approval.
Computer operations		
Low risk	**Medium risk**	**High risk**
Formal backup copying procedure does not exist. Formal responsibility for batch job monitoring/controlling is not assigned. Backup copies are not stored in a different type of data storage.	Backup copies are made too infrequently. No backup copies have been made in IS application level (to backup configured application settings). Data backup copies are kept in an inappropriate place. No restoration tests of the data backup have been regularly performed. Batch job logs are not controlled. Data backup logs are not controlled.	No data backup copies have been created. Disaster recovery plan (for IT) does not exist.
IT governance		
Low risk	**Medium risk**	**High risk**
IT documentation (IT security policy, internal procedures etc.) does not exist. IT documentation is not kept in an appropriate place. IT documentation is outdated.	Formal service level agreement (SLA) defining provided IT department services does not exist. Agreements with outsourced service providers are outdated.	Outsourced service providers' operations are not monitored and controlled.

Additionally, it is observed that in several organizations IT managers lack the knowledge of all IT department performed functions/administrated resources; IT environment controls are often made just before the audit (if audit is not made frequently, IT environment controls may be outdated); overall organizations' internal IT control maturity level is low, most often – 2 (according to COBIT (0 non-existent, 1 initial/*ad hoc*, 2 repeatable but intuitive, 3 defined process, 4 managed and measurable, 5 optimized)); better IT controls are present in banks, international corporations and companies that have implemented quality management systems.

V. The Analysis of the Research Results

To assess the need for IT control environment establishment, research data is analysed – 3 different types of organizations are compared: (1) organization group A – organizations without IT governance and without IT control environment; (2) organization group B – organizations with IT governance, without IT control environment; (3) organization group C – organizations with IT governance and IT control environment. In each group, 3 medium-sized organizations are selected. The results of comparison and analysis are summarized in risk maps. Risk maps show risks categorized and summarized by their areas (ITGC audited areas) according to their relative significance and likelihood and maps the risks into nine quadrants and three sectors. Position in the map (sector, quadrant) prioritizes the risks and indicates the level of concern and attention which should be directed toward mitigating risks. Sectors are divided using different colours – white, light gray and gray. White sector means that risks are rated "low", and they require minimal monitoring and control. Light gray sector means that risks are rated "moderate", and they should be monitored on a regular basis to ensure that they are appropriately managed. Gray sector means that risks are rated "extreme" and they should be reduced or eliminated immediately.

Fig. 4 shows the risk map and Table II describes the identified deficiencies, risks that can arise and risk area for organization group A.

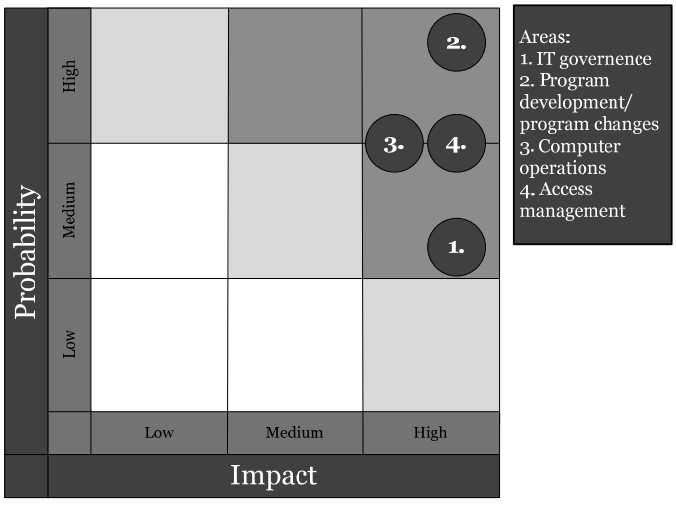

Fig. 4. Organization group A

TABLE II

IDENTIFIED DEFICIENCIES AND POTENTIAL RISKS TO ORGANIZATION GROUP A

Organization group A			
No.	**Identified deficiency**	**Potential risk**	**Risk area**
1.	Several unclosed user accounts (including administrator accounts) of organization ex-employees (in IS that processes financial data)	Unauthorised access to programs and data; Financial loss	4.
2.	IS that processes financial data is not secured with a password	Unauthorised access to programs and data; Financial loss	4.
3.	Server room does not have lock	Unauthorised access to programs and data; Data loss	4.
4.	Outsourced IS developers have full access to IS (that process financial data) production environment and their operations are not monitored/controlled by organizations' IT staff	Unauthorised access to programs and data; Financial loss	4.
5.	Data backup copies are kept in one room with servers without access control (no locks)	Data loss	3.
6.	No restoration tests of the data backup have been regularly performed, no evidence gained that data backup can be restored	Data loss	3.
7.	Changes to IS are not tested prior to implementation	Inadequate IS operation; Data loss or corruption	2.
8.	Agreement with outsourced IT manager is outdated, so he does not have legal responsibility about actions he made	Financial loss; Reputation loss	1.

Fig. 5 shows the risk map and Table III describes identified deficiencies, risks that can arise and risk area for organization group B.

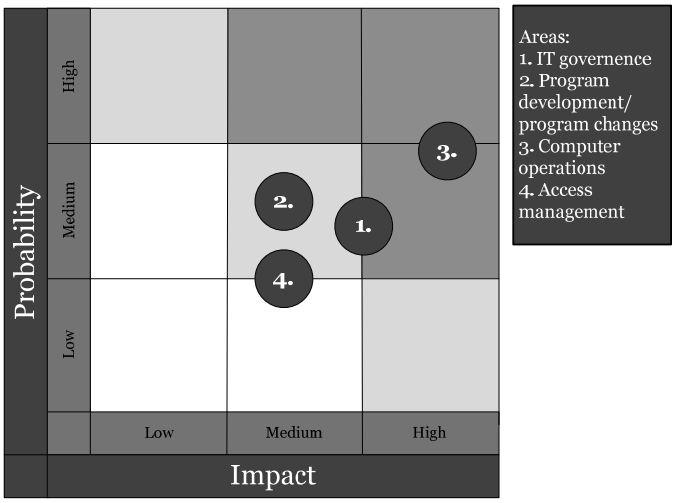

Fig. 5. Organization group B

TABLE III

IDENTIFIED DEFICIENCIES AND POTENTIAL RISKS TO ORGANIZATION GROUP B

Organization group B			
No.	**Identified deficiency**	**Potential risk**	**Risk area**
1.	Internal wireless network is encrypted with comparatively weak encryption protocol – WEP	Unauthorised access by a third party to programs and data	4.
2.	Server room is not appropriately equipped, the key is available to all organization's staff	Interruption of IT operation	4.
3.	IS that processes financial data password security settings are too weak in such positions: • minimum password length – 2 characters; • complexity requirements – disabled.	Data loss	4.
4.	Disaster recovery plan for IT operation restoration does not exist	Interruption of IT operation	3.
5.	IS test environment does not exist, changes are tested on IT developers' side, user acceptance testing is made in production environment	Inadequate IS operation; Data loss or corruption	2.
6.	Formally defined rules and responsibilities for IT personnel do not exist	Ineffective usage of resources; Financial loss	1.

Fig. 6 shows the risk map and Table IV describes identified deficiencies, risks that can arise and risk area for organization group C.

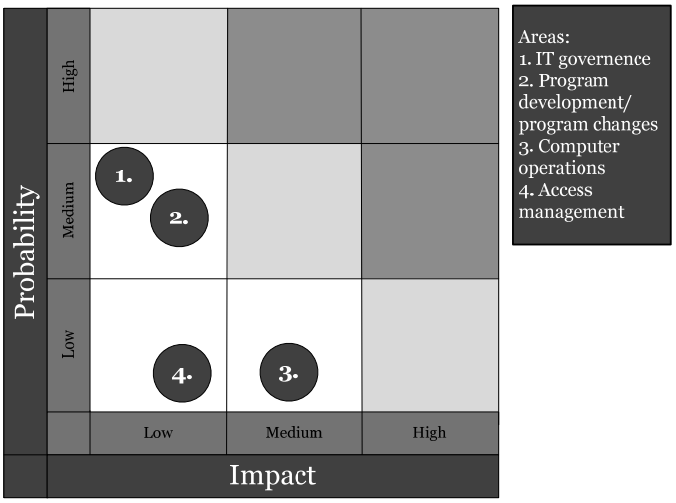

Fig. 6. Organization group C

TABLE IV
IDENTIFIED DEFICIENCIES AND POTENTIAL RISKS TO ORGANIZATION GROUP C

Organization group C			
No.	**Identified deficiency**	**Potential risk**	**Risk area**
1.	Administration procedure of written user access rights does not exist, administration process of formal user access rights exists, but it is not documented anywhere	Unauthorised access to programs and data	4.
2.	Backup copies are not stored in a different type of data storage	Data loss	3.
3.	IS changes are not documented in user manual, but IS usage trainings are made on a regularly basis	Inadequate IS usage	2.
4.	IT documentation is not freely available to all who need access to it	Ineffective usage of resources	1.
5.	IT documentation is outdated	Ineffective usage of resources	1.

Figures 4 and 6 show that for organization group C all risks are positioned in a white sector that means that risk level is rated "low", but for organization group A all risks are positioned in a gray sector, i.e., risk level is rated "extreme".

The analysis shows that during ITGC audit fewer deficiencies are identified for organization group C and risks are less significant. Also, the analysis shows that effective IT governance helps organizations reduce IT related risks, but without effective IT control environment significant risks still arise.

VI. CONCLUSIONS

The research shows that every year during the ITGC audit many deficiencies are found. Almost all organizations have potential risks that can arise from the identified deficiencies within user access rights management and computer operation areas and overall organizations' internal IT control maturity level being low. ITGC audit is very important to organizations because it can help reduce these risks and protect organizations from financial or reputation losses.

Research results provide evidence that organizations with the IT control environment (compared to organizations without the appropriate IT control environment) have fewer significant deficiencies and IT-related risks; potential impact and probability of identified risks are lower; the IT governance is on a higher level; IT operates more effectively helping organizations achieve the quality goals.

These observations suggest that the IT control environment helps organizations achieve better quality indicators and reduce the IT related risks.

These days, there are several standards and methodologies such as COBIT, ITIL and ISO 27001, 27002 that describe and give recommendations for IT control environment establishment. However, these standards and methodologies are designed for large organizations and frequently they need outsourced IT consultations to implement them. Further research will be continued in the IT control environment with the aim to develop simple understandable guidelines to IT control environment implementation and maintenance for medium-sized organizations in Latvia. It is planned to develop guidelines in the following IT control environment areas – IT governance, program development, program changes, computer operations and access to programs and data. The guidelines will include the recommended IT controls, support process descriptions (that can be easily adaptable to a specific organization) and documentation.

VII. REFERENCES

[1] S.-M. Huang, W.-H. Hung D. C. Yen, I.-C. Chang and D. Jiang, *Building the evaluation model of the IT general control for CPAs under enterprise risk management*, 2011.

[2] F. Gallegos and S. Senft, *Why Are Information Technology Controls and Audit Important?,* 2008.

[3] 360 GRC Whitepaper, *Sarbanes-Oxley (404) Network Assessment and Compliance*, 2010.

[4] S. Flowerday and R.V. Solms, *Real time information integrity = system integrity + data integrity + continuous assurances, Computers & Security*, 24 (8) (2005), pp. 604–613.

[5] C. Bellino, J. Wells, and S. Hunt, Enterprise Controls Consulting LP, *Auditing Application Controls,* 2007.

Ruta Pirta is a Master Student of Riga Technical University, at the program of Information Technology. She obtained her Bachelor degree (2009) in Electronic Commerce from Riga International School of Economics and Business Administration. She is currently working on her Master Thesis under supervision of Renāte Strazdiņa in the field of IT Control Environment establishment. The defence of the Master Thesis is planned to be held at the end of 2012.

She currently works as an IT Consultant at an international audit and consulting firm. E-mail: ruta.pirta@inbox.lv.

Renate Strazdina is a Leading Researcher at Riga Technical University, Department of System Theory and Design. She is a Doctor of Engineering Science since 2006 when she defended the Doctoral Thesis "Information System Feasibility Study in Turbulent Environment" at Riga Technical University.

Renate currently works as a Lecturer at Riga Technical University and Business and Executive Director at an international audit and consulting firm. Renate is a member of the Association of Chartered Certified Accountants and a member of program committees of different information system-related conferences. E-mail:renate.strazdina@cs.rtu.lv

Rūta Pirta, Renāte Strazdiņa. Informācijas tehnoloģiju vides kontroles nepieciešamības novērtējums
IT kontroles ir aktivitātes, ko veic sistēmas vai cilvēki, lai pārliecinātos, ka IT darbojas, lai atbalstītu biznesu un palīdzētu sasniegt organizācijas mērķus. IT kontroles vide ir savstarpēji saistītu kontroļu kopums, kas tiek piemērotas integrētai IT videi. IT kontroles ir definētas un aprakstītas vairākos starptautiskos standartos un metodoloģijās, piemēram, COBIT, ITIL un ISO 27001, 27002. IT kontroles vides audits tiek veikts IT audita ietvarā, kā arī finanšu audita ietvarā (lai iegūtu pārliecību par informācijas, ko apstrādā organizācijas izmantototās informācijas sistēmas, uzticamību). Empīriski novērojumi rāda, ka organizācijas bieži neievieš/neuztur atbilstošu IT kontroles vidi. Šajā pētījumā ir novērtēta IT kontroles vides nepieciešamība organizācijās, veicot IT kontroles vides audita datu analīzi (pētījuma ietvaros ir analizēti dati no IT kontroles vides audita (konstatētās nepilnības dažādos uzņēmumos), kas veikts ikgadējā finanšu audita ietvaros 61 uzņēmumā Latvijā) un intervējot nozares ekspertus (praktizējoši auditori, IT konsultanti, IT vadītāji). Pētījuma rezultātā secināms, ka uzņēmumos, kuros ir IT kontroles vide, salīdzinājumā ar uzņēmumiem, kuros nav atbilstošas IT kontroles, vides auditos ir konstatēts mazāk trūkumu, līdz ar to pastāv arī mazāk ar IT saistīto risku; konstatēto IT risku potenciālā ietekme un iespējamība ir zemāka; IT pārvaldība ir augstākā līmenī; no IT ir lielāka atdeve, kas palīdz sasniegt labākus kvalitātes rādītājus. No minētajiem secinājumiem izriet, ka efektīvas IT kontroles vides ieviešana organizācijās palīdzētu sasniegt labākus kvalitātes rādītājus tajās pamatdarbības jomās, kas ir atkarīgas vai cieši saistītas ar IT, papildus samazinot ar IT saistītos riskus.

Рута Пирта, Ренате Страздиня. Оценка необходимости управления средой информационных технологий
ИТ контроль это действия, которые осуществляются системой или людьми, чтобы убедиться, что IT работает с целью поддерживать бизнес и способствовать достижению целей организации. Средой ИТ управления являются набор взаимосвязанных контролей, которые применяются к интегрированной ИТ среде. ИТ контроли определены и описаны в нескольких международных стандартах и методологиях, например в таких, как COBIT, ITIL и ISO 27001, 27002. Аудит среды ИТ контроля проводится в рамках ИТ аудита и в рамках финансового аудита (для того, чтобы обрести уверенность в надежности информации, обрабатываемой информационными системами, которые используются в организации). Эмпирические наблюдения показывают, что организации зачастую не вводят/не поддерживают соответствующую среду ИТ управления. В данном исследовании оценивается потребность организаций в среде ИТ контроля, проводя анализ данных аудита среды ИТ управления (в рамках исследования анализируются данные с аудитов сред ИТ контроля, (недостатки обнаружены в различных компаниях), которые проводятся в рамках ежегодного финансового аудита в 61 латвийском предприятий) и проводятся интервью с экспертами отрасли (практикующие аудиторы, ИТ консультанты, ИТ менеджеры). Результаты исследования приводят к выводу, что на предприятиях, имеющих среду ИТ управления, по сравнению с компаниями, в которых нет среды ИТ контроля, в аудитах нашли меньше недостатков, поэтому там существует меньше рисков, связанных с ИТ; потенциальное влияние и вероятность рисков ИТ, которые определены, ниже; управления ИТ на более высоком уровне; отдача от ИТ больше, что помогает добиться лучших показателей качества. Из этих выводов следует, что эффективное внедрение среды ИТ контроля в организациях повышает качество работы в основных областях, которые зависят от или тесно связанны с ИТ, в дополнение к сокращению ИТ рисков.