Годишник Телекомуникации 2014, том 1, с. 119 - 125

Yearbook Telecommunications 2014, vol. 1, p. 119 - 125

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

РАЗРАБОТКА НА МОДЕЛ НА ИНТЕГРИРАНА ВЪТРЕШНА УПРАВЛЕНСКА СИСТЕМА (ИВУС) И АЛГОРИТЪМ ЗА ОЦЕНКА НА ОПЕРАТИВНАТА ЕФЕКТИВНОСТ

Кристиан Томов

DEVELOPMENT OF AN INTEGRATED INTERNAL MANAGEMENT SYSTEM (IICS) MODEL AND AN EFFICIENCY MEASUREMENT ALGORITHM

Kristian Tomov

Резюме: Много актуален е проблемът за създаване и внедряване на интегрирани вътрешни управленски системи (ИВУС) както в областта на телекомуникационните и информационни технологии, така и в други области. Използването на ИВУС е възможно и крайно необходимо решение на отворените въпроси спрямо ефективното управление особено на международни компании. В практиката на изследване, анализ и одитиране на ИВУС се използват много практически подходи, базирани на съответните стандарти.
В настоящата разработка се предлага модел на ИВУС, методика и алгоритъм за оценка на нейната оперативна ефективност.
Ключови думи: интегрирана вътрешна управленска система, управленска система, оценка на оперативната ефективност

Abstract: The issue of creating and implementing integrated internal management systems is very topical (IICS) for the governance of telecommunications and information technology structures . The use of an IICS for the corporate governance should be considered, as this would be an essential solution to the open questions on the efficient management especially in international companies. In the practice of research, analysis and audit of IICS many practical approaches based on international applied standards are used.
This paper proposes a IICS model, a methodology and an algorithm for the evaluation of its operating efficiency.
Keywords: integrated internal management system, management system, assessment of operational efficiency

1. ВЪВЕЖДАНЕ В ПРОБЛЕМАТИКАТА

Свидетели сме, че много от големите, преди години, организации в различните индустрии, са виждали късмета си да потъва, докато други си плуват на вълната на икономическия успех, водещ до растеж. „Управление, управление на риска и съответствието” е една от основните корпоративни програми, която трябва да бъде управлявана по подходящ начин [1]. Размишленията в книгата на Ричард Стейнберг посочват нуждата от акцент в сферата на вътрешното управление и, съответно нуждата от прилагане на интегриран управленски подход става видима. От това следва, че използването на интегрирана вътрешна управленска система (ИВУС) е възможно и крайно необходимо решение на отворените въпроси спрямо ефективното управление особено на международни компании.

В статията се описват резултатите от анализа на основната структура на ИВУС. Въз основа на предложен модел на ИВУС се разработва алгоритъм за оценка на тяхната оперативна ефективност, пряко свързан с оценката на функционирането на системата.

В предложения модел на ИВУС се използва модулен подход. Моделът включва общ модул (организационен), който се отнася до всички сфери на организационната управленска структура на предприятието. Включва също така и модули, които са

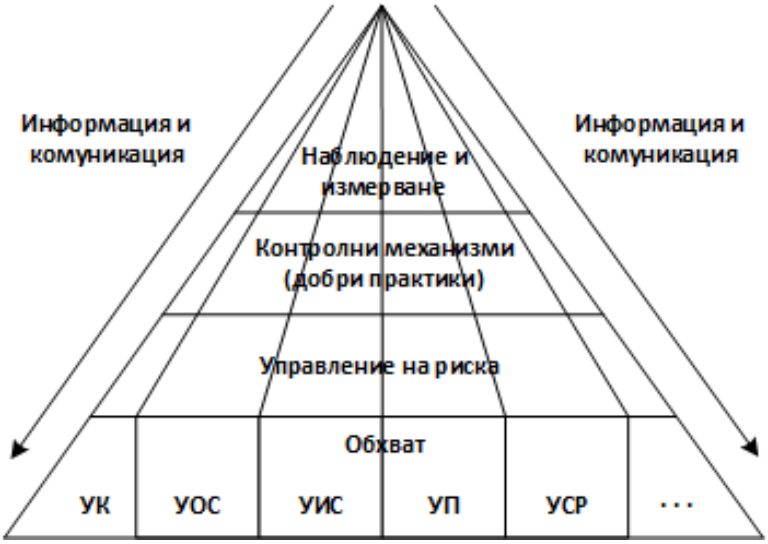
специфични, както и позволява възможни допълнения (модификации) чрез международно изпитани и проверени системи за управление. Към специфичните модули имат отношение, например: управление на качеството ISO 9001 [2], управление на околната среда ISO 14001 [3], управление на здравето и безопасността BS OHSAS 18001:2007 [4], управлението на риска ISO 31000 [5], управление на сигурността и управлението на информационната сигурност ISO/IEC 27001 [6], управление на процесите ISO 20000-1 [10], управление на извънредни ситуации ISO/IEC 22301 [8]/ BS 25999 [9].

Значимостта и актуалността на задачата за разработка на „алгоритъм за оценка на оперативната ефективност на ИВУС“ са обосновани не само от практиката на одиторската професия, както показват международно признатите дефинирани рамки, посочени в COSO [11] и ISO/IEC 27004:2009 [7] Information technology - Security techniques - Information security management - Measurement (стандарт за оценка в информационната сигурност от международната стандартизационна организация ISO), дадените насоки в нормите за вътрешен контрол в публичния сектор, или в международните разпоредби за финансово отчитане, като например SOX (Sarbanes-Oxley Act), също от друга страна в директивите на ЕС и т.н.

Важно изискване към разработвания алгоритъм е да бъде широко приложим и да позволява оценка на оперативната ефективност на ИВУС спрямо изискванията към нея и вложените в нея инвестиции. Такива системи са вече внедрени в частния сектор, както и в организации от публичния сектор.

2. ОСНОВНА СТРУКТУРА НА МОДЕЛА НА ИВУС

Като се вземат под внимание постановките на описаните в т. 1 стандарти, както и опита от практиката, въз основа на техния детайлен анализ, може да се предложи обобщен управленски модел. Предлаганият модел на ИВУС има основна структура, показана на фиг. 1. Както беше казано, използва се модулен подход, което позволява непрекъснато разширение, модифициране и адаптиране на ИВУС. Обхватът на всяка конкретна ИВУС зависи от нуждите на съответната фирма.



Фигура 1. Структура на предлагания модел на ИВУС.

На фиг. 1 е показан и обхватът на прилагане на отделните сфери в схемата на модела на ИВУС, както следва (отворен е за разширение):

УК - управление на качеството;
УОС - управление на околната среда;
УИС - управление на информационната сигурност;

УП - управление на процесите на взаимодействие;

УСР - управление на сигурността по време на работа;

. . . - управление на непрекъсваемостта и управление на съответствието спрямо законодателството (за определените сфери);

Информация и комуникация – посока на движение на информацията и комуникацията.

Последователността от стъпки, за да се осигури изискваната функционалност на системата, е следната:

1. Обхват - обхватът включва всички организационни и специфични управленски дейности (съгласно т. 1), които са приложими в компанията спрямо нейните операции. Обхватът се определя от индивидуалните изисквания на системата за управление.

2. Наблюдение и оценка – извършва се непрекъснато наблюдение и оценка на параметрите на ИВУС от старшия управленски състав. Това включва вътрешно одитиране, документиране на резултати, наблюдение и оценка на тяхното развитие, както и оценка на тяхната оперативна и финансова ефективност.

3. Контролни механизми (добри практики) – съвкупност от организационни и технически контролни механизми (превантивни, детективни и коректривни), използващи приети добри практики.

4. Управление на риска – модел за управление на цялостния корпоративен риск (съгласно формулировката на задача 3).

5. Информация и комуникация - необходимата контролна информация и комуникационни канали.

Въз основа на предложения модел, дадена ИВУС е готова за внедряване, с определена в зависимост от конкретния клиент организационна структура, от неговата основна дейност, а също и от други изисквания, специфични за сектора. Следващата възможна стъпка е сертифицирането на тази ИВУС, съгласно изискванията, тъй като тя е построена в съответствие с приложимите технически стандарти и включва всичко необходимо за тази цел. Значението на сертификацията се заключава във възможността за периодични проверки на функционирането от трета страна. Тъй като това е свързано с разходи, разбира се, е необходимо да се извършва непрекъсната оценка на оперативната ефективност на ИВУС.

Предложеният модел е валиден при следните **ограничителни условия**:

- моделът се отнася изключително за управление на корпоративни структури в областта на информационните и телекомуникационни технологии;

- моделът е разработен с достатъчна степен на общност на параметрите, като същевременно позволява множество от конкретни интерпретации, всяка от които е уникална за всяка структура. Параметрите могат да приемат два типа стойности - опционални и изискуеми. Моделът изисква калибриране чрез конкретната интерпретация, конкретните условия и вида на продукта/услугата;

- моделът не включва управление на финансите и на научно-изследователската и развойна дейност;

- моделът се ограничава строго до добрите практики, които са въз основа на ISO стандартите, както и на ITIL v2 и v3 (Information Technology Infrastructure Library), CCTA (Central Computing and Telecommunications Agency (CCTA), Cabinet Office, part of Her Majesty's Government (HMG)), и на eTom (ITU);

- моделът е строго управленски и в резултат дава управленската рамка, като не включва техническата реализация на съответните механизми.

3. АЛГОРИТЪМ ЗА ОЦЕНКА НА ОПЕРАТИВНАТА ЕФЕКТИВНОСТ НА ИВУС

На база на анализа на функциониране на модела на ИВУС (съгласно т. 2), може да се предложи разработен алгоритъм за оценка на нейната оперативна ефективност.

В т. 2 (фиг. 1) е показана основната структура на ИВУС. На най-високото ниво на пирамидата (управленско ниво) е параметърът "Наблюдение и измерване".

Въз основа на това описание е предложен аналитичен модел и алгоритъм за оценка на оперативната ефективност на ИВУС. Моделът е базиран на следните предложения:

- Предлага се създаване на контролни групи (например група за kg_f, показана по-долу), които съдържат определени контролни механизми, всеки от които е в съответствие с типа на контролата (превантивна, детективна и коригираща). Контролни групи се създават за всяка заплаха (списък рискове), описани съгласно конкретния случай на приложение.
- Предлага се оперативната ефективност на ИВУС да се определя от средната стойност на ефективността на контролните групи (E_{iks}).

Като се вземат под внимание горните предложения, методиката за определяне на оперативната ефективност на E_{kg} се дефинира в аналитичен вид за различните случаи както следва:

$N_i = 0$ $E_{kg}=K1$ (в случай, че няма установени инциденти);

$N_i \neq 0$ $t_{di} \leq t_d$ and $t_{fi} \leq t_f$ $E_{kg}=K2$ (в случай, че превантивните контролни механизми не са сработили, но детективните и коректривните контролни механизми са сработили (в определените им времена за реакция));

$N_i \neq 0$ $t_{di} > t_d$ and $t_{fi} \leq t_f$ $E_{kg}=K3$ (в случай, че превантивните и коригиращите контролни механизми са сработили, но превантивните контролни механизми не за определеното време за реакция, а коригиращите са сработили в определеното им време за реакция);

$N_i \neq 0$ $t_{fi} > t_f$ $E_{kg}=K4$ (в случай, че превантивните и детективните контролни механизми не са сработили, а коригиращите контролни механизми са сработили, но не за определеното време за реакция).

В методиката са използвани следните обозначения, заедно с ограничителните условия:

- kg - Контролна група / задача група,
- E_{kg} - Ефективност на контролна група,
- E_{iks} - Ефективност на ИВУС,
- N_i - Инциденти по сигурността,
- t_d - Дефинирано време за откриване на инцидента,
- t_f - Дефинирано време за премахване на инцидент,
- t_{di} - Време на възникване на инцидента по сигурността,
- t_{fi} - Реално време за премахване на инцидент по информационна сигурност.

Ограничителни условия:

1. Авторът приема четири случая и съответно приема четири константи K_i като гранични стойности.
2. Авторът приема стойности на въведените константи като гранични стойности, както следва: К1=100%, К2=80%, К3=50% и К4=0%.

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

Тези ограничителни условия се базират на постановката описана в ISO/IEC 27004:2009, че нивото на грануларност и съответното детайлизиране на оценката на ефективността се определя от компанията прилагаща такъв модел. Поради това се определя минимално ниво за оперативна ефективност на ИВУС със стойност 80 %, т.е. приетите стойности на приетите константи К1 и К2 не трябва да имат резултат под 80% ефективност спрямо всяка отделна контролна група. В противен случай, естествено, не може да се приеме за приемливо твърдението, че ИВУС е оперативно ефективна.

Описаната методика предвижда създаване и на съответен алгоритъм за оценка на оперативната ефективност на ИВУС, както следва:

$$Kg = \{if\ (Ni = 0)\ then\ Ekg = 100\%, else, if\ (tdi \leq td\ and\ tfi \leq tf)\ then\ Ekg = 80\%\ else\ if\ (tdi > td\ and\ tfi \leq tf)\ then\ Ekg = 50\%\ else\ if\ (tfi > tf)\ then\ Ekg = 0\%\}$$

Съгласно предложения алгоритъм, всяка компания, която го прилага, е необходимо да предостави дефиниран списък на типовете инциденти и контролни изисквания (времена за реакция) на ИВУС.

4. ПРИМЕР ЗА ПРИЛАГАНЕ НА АЛГОРИТЪМА ЗА ОЦЕНКА НА ОПЕРАТИВНАТА ЕФЕКТИВНОСТ НА ИВУС

Примерът използва постановката, показана в т. 3.

Примерни рамки за категоризиране

ИВУС изисква индивидуален анализ на корпоративните структури и техните оперативни дейности. Чрез анализа се дефинират константи и дефиниции за типовете инциденти, контролните изисквания спрямо управленската система и създаването на контролни групи. В случая е развита една заплаха („пожар”) с цел доказване на алгоритъма, като в реални обстоятелства се използва списък от заплахи (пример за такъв списък може да бъде намерен например в:

http://www.symantec.com/security_response/landing/azlisting.jsp).

Типове инциденти

Категоризацията на типовете инциденти спрямо щетите от въздействието на заплаха върху операциите в съответна компания е показана в табл. 1.

Таблица 1. Категоризация на типовете инциденти.

Тип инцидент	Дефиниция
Критични	< 1 M Euro
Средни	> 1 M Euro
Стандартни	> 50 K Euro

Контролни изисквания

Категоризацията на изискванията за времената на реакция на контролните механизми, част от ИВУС, спрямо щетите от възможни въздействия на възникнала заплаха върху операциите на съответната компания е показана в табл. 2.

Таблица 2. Категоризация на изискванията за времената на реакция на контролните механизми.

Тип инцидент	**Тип контрола**	**Изисквания (KPI -** Key Performance Indicator**)**
Критични	Превантивни	0
	Детективни	$t_d \leq 0{,}5$ сек.
	Коригиращи	$t_f \leq 10$ сек.
Средни	Превантивни	0
	Детективни	$t_d \leq 0{,}9$ сек.
	Коригиращи	$t_f \leq 1{,}5$ мин.
Стандартни	Превантивни	0
	Детективни	$t_d \leq 2{,}0$ мин.
	Коригиращи	$t_f \leq 10{,}5$ мин.

Създаване на контролни групи

В случая се създава контролна група за контрол на заплаха „пожар“, показана в табл. 3.

Таблица 3. Категоризация на изисквания за реакция на контролните механизми.

Риск	**Контрола**	**Тип контрол**	**Група контроли**
Пожар	Кодекс за поведение, директива за поведение по време на пожар, обучение за защита от пожари.	Превантивни	kg_f (контролна група - пожар)
	Детектори на дим, VESDA (Very Early Smoke Detection Apparatus – Апарат за ранно разпознаване на дим).	Детективни	
	Автоматично пожарогасене, план за възстановяване на инфраструктурата.	Коригиращи	

5. ЗАКЛЮЧЕНИЕ

В практиката на изследване, анализ и одитиране на ИВУС се използват много практически подходи, базирани на съответните стандарти.

В настоящата разработка е предложен обоснован модел на ИВУС, описана е методика и е предложен алгоритъм за оценка на нейната оперативна ефективност, пряко свързан с оценката на нейното функциониране. Използван е модулен подход и са дадени ограничителни условия.

Представените резултати в разработката могат да бъдат широко приложими и да позволяват оценка на оперативната ефективност на ИВУС спрямо изискванията към нея и вложените в нея инвестиции. Такива системи са вече внедрени в частния сектор, както и в организации от публичния сектор.

Като една възможност за продължение на тази разработка може да се предложи приложението на алгоритъма и доказване на ефективността в реални условия.

ЛИТЕРАТУРНИ ИЗТОЧНИЦИ:

[1] STEINBERG, Richard M. *Governance, Risk Management, and Compliance: It Can't Happen to Us--Avoiding Corporate Disaster While Driving Success*. Wiley, 2011. ISBN 978-1-118-02430-0.

[2] ISO 9001:2008 Системи за управление на качеството. *AQ Cert* [онлайн]. [прегледан 23 април 2013]. Достъпен на: https://www.aqcert.org/ ; ISO 9001:2008 Quality management systems - Requirements
[3] ISO 14001. *Евро стандарт сертификация ЕООД* [онлайн]. [прегледан 13 април 2013]. Достъпен на: https://escert.com ; Environmental management systems - Requirements with guidance for use и ISO 14004 Environmental management systems - General guidelines on principles, systems and support techniques
[4] BS OHSAS 18001:2007 Система за управление на здравето и безопасността при работа. *Евро стандарт сертификация ЕООД* [онлайн]. [прегледан 13 април 2013]. Достъпен на: https://escert.com ; BS OHSAS 18001:2007 occupational health and safety management systems
[5] ISO 31000:2009 Risk management – Principles and guidelines. *International Organization for Standardization*. [online]. [viewed 23 April 2013]. Available from: https://www.iso.org
[6] ISO/IEC 27001:2013 Система за управление на информационната сигурност. *Евро стандарт сертификация ЕООД* [онлайн]. [прегледан 13 април 2013]. Достъпен на: https://escert.com ; ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements
[7] ISO/IEC 27004:2009 Information technology - Security techniques - Information security management – Measurement. *International Organization for Standardization*. [online]. [viewed 23 April 2013]. Available from: https://www.iso.org
[8] ISO 22301:2012 Societal security - Business continuity management systems – Requirements. *International Organization for Standardization*. [online]. [viewed 23 April 2013]. Available from: https://www.iso.org
[9] BS 25999-1:2006 Business Continuity Management. Part 1: Code of practice. *ENISA* [online]. [viewed 22 April 2013]. Available from: https://www.enisa.europa.eu
[10] ISO/IEC 20000-1:2011 Information technology - Service management - Part 1: Service management system requirements. *International Organization for Standardization*. [online]. [viewed 23 April 2013]. Available from: https://www.iso.org
[11] *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*. [online]. [viewed 23 April 2013]. Available from: https://www.coso.org

Информация за автора:
Маг.-инж. Кристиан Томов, докторант, Департамент ”Телекомуникации” на НБУ, ул. Монтевидео № 21, 2-609, Тел.: 359 2 8110609, e-mail: kristiantomov@yahoo.com

Contacts:
MSc Kristian Tomov, Postgraduate, Department Telecommunications, 21 Montevideo St., 2-609, Tel: 359 2 8110609, e-mail: kristiantomov@yahoo.com.

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 20.07.2014
Дата на приемане за публикуване (Date of adoption for publication): 02.09.2014