НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ

Департамент „Телекомуникации“

маг. инж. Кристиан Димитров Томов

АНАЛИЗ И ОПТИМИЗИРАНЕ НА ВЪТРЕШНИ КОНТРОЛНИ СИСТЕМИ В ТЕЛЕКОМУНИКАЦИОННИ СТРУКТУРИ

АВТОРЕФЕРАТ

на дисертация

за придобиване на образователна и научна степен

„ДОКТОР“

по научна специалност
„Комуникационни системи и мрежи“

в професионално направление
5.3. „Комуникационна и компютърна техника“

Научен ръководител

доц. д-р Васил Къдрев

гр. София, март 2016 г.

Дисертационният труд е обсъден и предложен за защита на заседание на Департаментен съвет на департамент „Телекомуникации” към НБУ, проведено на 05.02.2016 г. (Протокол № 60).

Данни за дисертационния труд:

Брой страници: 119

Брой литературни източници: 103

Брой публикации по темата на дисертационния труд: 10

Номерацията на фигурите и таблиците в автореферата е същата като в дисертацията.

Защитата на дисертационния труд ще се състои на 18.07.2016 г. от 10:30 ч. в зала 607 на корпус 2 на НБУ, на открито заседание пред научно жури, назначено от ректора на НБУ.

Материалите по защитата са на разположение на заинтересованите в департамент „Телекомуникации”, корпус 2, офис 609 и на Интернет страницата на НБУ.

Автор: маг. инж. Кристиан Димитров Томов

Тема: „Анализ и оптимизиране на вътрешни контролни системи в телекомуникационни структури”

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

Телекомуникационната структура е многокомпонентна система, състояща се от съоръжения, човешки ресурси, технологии и връзки, чрез които се създават и предоставят телекомуникационните услуги, използващи обмен на информация. Този процес на предоставяне чрез информационните и комуникационни технологии на услуги посредством ресурсите на телекомуникационните структури (информацията, съоръженията, технологиите, човешките ресурси и връзките) изисква интегрирани управленски системи (ИСУ).

Система за управление (СУ) е рамка с организационни и технически контролни механизми за управление на специфична сфера (под „сфера" се има предвид съвкупността от спомагателни процеси за непрекъснато предоставяне на информационни и комуникационно-технологични (ИКТ) услуги) на организация и нейния бизнес (т. нар. „средства за мениджмънт"). ИСУ е интеграция на няколко системи за управление с цел оптимизация на ефективността на процесите и операциите, доставка на качествени и сигурни услуги, пазенето на собствените човешки ресурси и др. ИСУ се състои от голям брой технически и организационни контролни механизми (пример за технически това е антивирусен софтуер, пример за организационни е наредба за работа с технически активи на организацията и т.н.) за постигане на максимално качество, сигурност, непрекъсваемост на бизнеса, както и други оперативни цели, предоставящи възможността за непрекъснато подобрение на бизнеса. Отпадането на който и да е контролен механизъм би могло да доведе до колапс на цялостното доставяне на услугата и пряко негативно влияние върху потребностите на клиентите.

Една пряка съпоставка между неуспешните телекомуникационни компании и успешните компании показва голямата разлика в оперативната ефективност на подходите за управление. Оперативната ефективност на СУ се определя главно от нивото на интеграция между единичните компоненти на системата и нивото на внедряване на съответните контролни механизми в специфично-оперативния бизнес. Голяма част от телекомуникационните структури се опитват да преминат от реактивния и сегрегиран (няма СУ и ИСУ) към проактивния и интегриран (ИСУ) подход. С други думи - реагира се в момента, в който отпада услуга/процес, не се анализира коренната причина и не се правят изводи, за да се достигне значително ниво на непрекъснато подобряване на компанията.

Трудно бихме си представили живота в 21-ви век без информация и комуникация, както и без използването на ИКТ (информационни и комуникационни технологии). Поради това защитата и мениджмънта на телекомуникационните среди става все по-важна.

Визията за интеграция на системи за управление във вид на интегрирани системи за управление за първи път се среща в анекс (Annex SL), част от директива на международната организация за стандартизация. Той изисква унифициране на изискванията при създаване на управленски стандарти (т.е. тяхното „стандартизиране") във всички сфери с цел да се позволи лесна интеграция между различните системи за управление. Детайлно описване на интердисциплинарни управленски системи обаче няма като публична информация, тъй като те са скъпо платено знание на всяка една международно активна и успешна организация (това се вижда и от направения литературен обзор).

На практика обикновено е трудно да се създаде и да се поддържа адекватно ниво на ИСУ. Причините за това са много - липса на ресурси, ниска осъзнатост за иновация (колкото по-голяма е една организация, толкова по-голяма нужда има от оперативно ефективна ИСУ, но колкото е по-голяма, толкова по-трудно се постига желаната промяна), ограничени бюджети и не на последно място увеличаващата се сложност в организацията на съвременните компании – дейността им, комуникацията и предоставянето на техните услуги. Много на брой консултанти в тази област предлагат различни решения и продукти за внедряване на СУ (например само за система за управление на сигурността има над 30 варианта на национални и международни стандарти). Дори експертите имат проблеми с проследяването на надеждността на тези предложени решения за изграждане, внедряване и поддържане на СУ.

Качеството и сигурността по време на работа, опазването на околната среда и сигурността на информацията е основна необходимост за успешен и дългосрочен бизнес, тъй като потребителите и служителите на организациите се развиват и осъзнават правата си и съответно повишават изискванията спрямо снабдителните организации. В епохата на глобализация и нарастваща мобилност се повишава зависимостта на индустриализираните нации от информационните и комуникационните технологии и тяхното качествено и сигурно предоставяне. Това кара телекомуникационните организации да вземат много на брой мерки, които ако не са координирани правилно, не биха били успешни.

Успешното управление на организациите в глобализирания свят изисква ефективен, ефикасен и гъвкав управленски подход. Ефективността може да се търси в контекста на корпоративното управление и третиране на рискове съвместно с всички заинтересовани страни. Понятието "ефикасно" означава, че необходимите задачи са завършили успешно с минимално използване на ресурсите. Изискването за гъвкавост позволява на компанията да бъде в състояние лесно да отговори на променящите се условия и нови изисквания.

В настоящата дисертация се представят основните моменти в анализа на изграждането на т. нар. „интегрирана вътрешна управленска система (ИВУС)[1]", понятие което се въвежда за пръв път и е основен обект на приложимостта на дисертацията. В това понятие задължително са включени някои от най-добрите международни практики при изграждането на ИСУ. Разработената ИВУС е въз основа на: стандарти за качество (стандарт ISO 9001), безопасност по време на работа (стандарт OHSAS 18001), околна среда (стандарт ISO 14001) и информационна сигурност (стандарт ISO 27001). Процесът на създаване и изследване на приложимостта на ИВУС представлява процес на анализ и оптимизиране на вътрешни контролни системи в телекомуникационни структури.

Разработката включва следните акценти: необходимост от разработване и внедряване на ИВУС; същинска реализация на ИВУС, методи за управление на риска чрез ИВУС; измерване на оперативната ефективност на ИВУС.

В тази връзка се представят някои методики и алгоритми за използване на цялостния модел на ИВУС. Алгоритъмът представя логическия процес по който се реализира и функционира модела.

ИВУС е отговорна за управлението и надзора на комплексни организации. Тя включва поредица от процеси и интегрира всички аспекти на бизнеса, като например управление на тези процеси, осигуряване на качеството, опазване на околната среда и

[1] IICS – Integrated Internal Control System.

безопасност на труда, управление на извънредни ситуации, сигурността, както и много други, събрани в единна управленска структура. Изследванията са проведени чрез създаване на модел на ИВУС, с отчитане на условията на функциониране, като е предвидена възможността за използване на различни варианти.

Цели и задачи на дисертационния труд

В съответствие с направения критичен анализ на приложението и ефективността на вътрешните управленски системи на телекомуникационни структури, **целите** на дисертационния труд се формулират така:

- Изследване и анализ на необходимостта на ИВУС (Интегрирана Вътрешна Управленска Система).
- Разработка на модел на ИВУС на база управление на качеството, околна среда, сигурността по време на работа и информационна сигурност, разработка на съответен алгоритъм за управление на риска и изследване на параметрите на оперативната ефективност на ИВУС.
- Анализ и разработка на модел и алгоритъм за внедряване на ИВУС.

За постигане на тези цели трябва да се разработят следните задачи:

1. Да се изследва необходимостта от ИВУС.
2. Да се разработи модел на ИВУС.
3. Да се разработи алгоритъм за управление на риска, включващ идентифициране на критични активи, групиране на активи, прилагане на стандартен списък от контроли чрез анализ на необходимостта от защита на активите, както и създаване на разширена методика за оценка на риска, въз основа на модел на ИВУС.
4. Да се разработи модел и алгоритъм за измерването на оперативната ефективност на ИВУС, включващ критерии за оценка на оперативната ефективност на ИВУС на база на примерни контролни групи и контролни механизми, взети под внимание в процеса на третиране на рисковете след извършване на разширената им оценка.
5. Да се разработи метод и алгоритъм за внедряване на ИВУС, въз основа на подход, включващ система за управление на качеството, система за управление на информационната сигурност, система за управление на здравословните и безопасни условия на труд и система за управление на околната среда.

Публикации по дисертацията

Във връзка с дисертационния труд са направени 10 научни публикации. От тях 4 на национални конференции с международно участие (1 публикация в Телеком 2012, 2 публикации в Телеком 2013, 1 публикация в АСТЕЛ 2013), 1 публикация в международна регионална конференция на ITU, 2 публикации в международно електронно научно-технологично издание (http://www.all-about-security.de) и 3 публикации в Годишник на департамент „Телекомуникации” от 2014 г.

Има едно забелязано цитиране на научна публикация на маг. инж. Кристиан Томов.

Структура и обем на дисертационния труд

Дисертационният труд включва увод, пет глави, заключение, списък на използваната литература, списък на авторските публикации, списък на съкращенията. Изложението на дисертационния труд е оформено в 119 страници. Използвани са 103 литературни източника.

II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

ГЛАВА 1. ЛИТЕРАТУРЕН ОБЗОР И АНАЛИЗ НА СЪВРЕМЕННОТО СЪСТОЯНИЕ

Ползите от изграждане, внедряване и поддържане на ИСУ в телекомуникационните структури са значителни. Чрез интеграция на функциониращи отделни системи за управление се постига по-висока ефикасност на процесите, намалява се бюрокрацията, оптимизират се комуникационните канали, както и се постигат много добри нива на управление на процеси и дейности, попадащи под регулаторни изисквания – околна среда, здравословни и безопасни условия на труд, сигурност на данни и информация и др.

Предвид сферата на дейност, телекомуникационните структури е препоръчително да бъдат сертифицирани по няколко международни стандарти. Това са ISO 9001, поставящ основите на управлението на качеството; ISO 14001, посочващ изискванията за изграждане на система за управление на околната среда, OHSAS 18001, определящ специфичните изисквания за работа с цел гарантиране на безопасността и здравето на работниците, както и ISO 27001, определящ критичните контроли.

Начините за интегриране на отделните системи за управление са много. Наименованието ИСУ е прието като общо описателно понятие за няколко различни системи за управление, които са интегрирани в една. Въпреки това, не е ясно доколко ИСУ в една организация е наистина интегрирана, тъй като не е определена ясна рамка, въз основа на която системите следва да бъдат интегрирани.

Настоящият труд включва основната част, касаеща ефикасното интегриране на различни СУ, която според автора все още не е надлежно документирана, а именно матрица (модел на ИВУС), която обхваща основните елементи от всеки стандарт, сравнява го със сходни елементи от другите стандарти и визуализира един завършен модел, въз основа на който организацията е препоръчително да изгради документацията на системата. Именно чрез използването на този модел, интегрираната система може да придобие един унифициран вид и да се превърне в ИВУС.

Изграждането на ИВУС, използвайки модела на ИВУС, описан по-долу в настоящата разработка, създава една цялостна система, изградена с ясни логически връзки, прозрачна, оптимизирана и най-вече гъвкава и лесна за поддръжка.

Неразделна част от ИВУС е измерването на ефективността, управлението на риска. В настоящата работа тези направления са силно застъпени, тъй като според автора те са в основата на функционирането на една ефективна, ефикасна и рисково ориентирана система.

Приноси към първа глава

Въз основа на изготвения критичен анализ могат да бъдат направени следните **изводи:**

- Понятието ИВУС представя необходима система за управление, интегрирана с помощта на специфично изготвен модел и структура.
- Целта на използването на модела на ИВУС е стандартизиране на процеса по интеграция с цел ефективност и ефикасност.
- Изграждането на ИВУС създава една цялостна прозрачна система включваща ясни логически връзки, гарантираща ефикасност и оптимална функционалност на процесите.

Приноси от първа глава:

1.1. Направен е критичен анализ на въпросите свързани с управленски системи въз основа на разгледаната литература.

1.2. Уточнени са целите и задачите на дисертацията.

ГЛАВА 2. АНАЛИЗ И СИНТЕЗ НА МОДЕЛ НА ИВУС

2.1. Дефиниране на условията за създаване на интегрирана управленска система

Понастоящем бизнес светът непрекъснато се променя и всеки ден става по-сложен и по-комплексен. По своята същност, той е изпълнен с риск. Исторически погледнато, фирмите са гледали на риска като на необходимо зло, което трябва да бъде сведено до минимум или смекчено, когато това е възможно. Едно от съществените условия за създаване на интегрирана управленска система, това е отчитане и оценка на риска.

Правилно съставена, оценката на риска дава на организациите ясна представа за състоянието на рисковете в бизнес процесите, независимо дали са вътрешни или външни, непосредствено предстоящи или по-далеч напред в бъдещето. Една добра оценка е „закотвена" в апетита към риск на организацията, което осигурява база за определяне на рискови реакции.

Управлението изисква внедряване и поддържане на необходимия контрол във всички сфери на бизнеса (процеси, качество, околна среда, сигурност, производство и др.), за да се гарантират качествени и ефективни операции с едновременно спазване на регулаторните изисквания [А4].

В момента не съществува подобен общоприет стандарт, който би подкрепил една компания в изграждането на ИСУ и/или при управлението на риска. Въпреки това компонентите на системата за управление може да се сравняват помежду си.

От страна на ISO има опити за стандартизирането на управленски стандарти чрез директива „ISO/IEC Directives, Part 1 Consolidated ISO Supplement - Procedures specific to ISO, Proposals for management system standards", при което се изисква еднакъв подход и структура по отношение на всички нови или намиращи се в преработка стандарти. В бъдеще всички стандарти за системи за управление на ISO следва да бъдат съгласувани и съвместими.

Понастоящем смислена интеграция на системи за управление в дадено предприятие може да бъде дефинирана и направена само специално за бизнеса на тази компания.

Например контролираните параметри на риска при системи за управление с PDCA цикъл, могат да се постигнат чрез въвеждането на мерки, в т.ч. изискването за непрекъснато усъвършенстване и оценка на риска, както и подобряване на някои параметри като качество, околна среда, безопасност и др.

Връзката между заинтересованите страни и ключовите изисквания на ИСУ са дадени като пример в таблица 2.1 (за всяка компания се разработва конкретен вариант).

2.2. Предпоставки и критерии за разработка на ИВУС

Интегрираната вътрешна управленска система (ИВУС) [А1] ще се използва за управление на телекомуникационната структура в сферата на качество, безопасност по време на работа, управление на околната среда, процесите и сигурността. Моделът на ИВУС съдържа организационни (административни) и технически, превантивни, детективни и коригиращи изисквания (механизми за контрол) спрямо телекомуникационната структура, както и препоръка за изпълнението им.

Моделът за управление на телекомуникационна структура чрез интегрирана вътрешна управленска система включва метод за идентификация и прилагане на подобни контроли в оперативната дейност.

Превантивните механизми за контрол (организационни или технически) имат за цел предварително да ограничат прерастването на риска в събитие, което е неблагоприятно за постигането на целите на предприятието. В тази връзка необходимите понятия могат да се дефинират както следва:

Таблица 2.1. Връзка между заинтересованите страни и ключовите изисквания към ИСУ които са включени към ИВУС.

	Отчетността	**Прозрачност**	**Етика**	**Ефективна икономичност**	**Сигурност по време на работа**	**Качество**	**Околна среда**	**Сигурност**
Собственик				X				X
Служител					X			X
Доставчик	X	X	X					X
Клиент	X		X			X	X	X
Потребител	X					X		X
Съседи			X				X	
Общности		X	X	X			X	X
Правителство		X	X	X	X		X	X
Органи на реда		X	X		X		X	X
Природа		X	X				X	

- Детективните механизми за контрол са механизми (организационни или технически), които трябва да въздействат на съответно събитие, преди (често е определено времето за реакция) то да е нарушило постигането на целите на предприятието;
- Коективните механизми за контрол са механизми (организационни или технически), които трябва да коригират причинените отклонения от нормалните оперативни дейности и свързаните с тях корпоративни цели;
- Ефективността в контекста на ИВУС е окачествяване на оперативна дейност. Ефективната оперативна дейност е оптимално администрирана, регламентирана, наблюдавана, непрекъснато подобрявана и извършвана дейност. За да се твърди, че съответната ИВУС е ефективна, трябва да има добре сработени и функциониращи механизми и процеси, чрез които да се постигат корпоративните цели;
- Надеждността е способността на обекта да запазва във времето стойностите на всички параметри (в установените граници), характеризиращи възможността му да изпълнява изискваните от него функции в зададени режими и условия на използване, техническо обслужване, ремонт, съхранение и транспортиране;
- Безопасност – това е състояние, при което с определена вероятност се изключва появяването на опасности. Безопасността е защитно състояние на обекта, при което въздействията не превишават максимално допустимо значение. Във връзка с безопасността се дефинират опасно и защитно състояние на системата. От друга

страна безопасността в европейските норми се дефинира като отсъствие на недопустим риск. Безопасността е понятие свързано с надеждността чрез събитието „отказ" на обекта. Безопасността не е „чист" продукт на надеждността, не произтича единствено и само от нея и не е неин частен случаи. В смисъл на надеждност, безопасността включва само последиците на отказа и зависи само от вредните (опасните) им въздействия върху обслужващия персонал и околната среда;

- Опасност - ситуация в заобикалящата ни природа или производствена среда, в която при определени условия е възможно възникването на нежелани събития или процеси (опасни фактори) въздействието на които върху човека и околната среда може да доведе до едно или съвкупност от следните въздействия:
  - Авария или катастрофа в техносферата;
  - Нарушения в състоянието на околната среда;
  - Отклонения в здравето на човека от средно статистическото значение.

Опасността е от категорията на вероятностите, която може да се променя в пространството и времето. Под характеристики на опасността, свързани с конкретно събитие, се разбира вероятността за появяване на това събитие на дадено място и за дадено време.

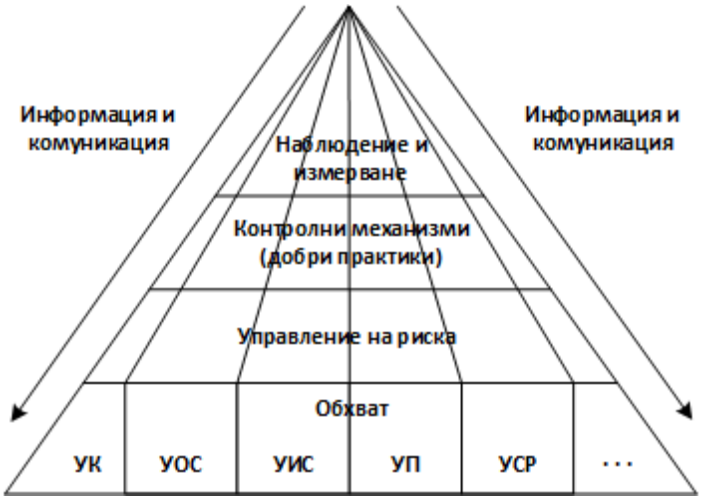
Рискът при използването на техническите обекти е равнозначен на изискването за безопасност при тяхната експлоатация. Категорията на „риска" се представя не само от понятието „опасност", но и от понятието „уязвимост". Уязвимостта характеризира загубата на устойчивост (защита) на обектите (субектите), към оказваните от него неблагоприятни въздействия. Наличието на опасност и уязвимост са необходими и достатъчни условия за възникването на риск.

Рискът се определя както качествено, така и количествено. Рискът количествено се определя като честота (вероятност) за възникване на едно събитие (авария, инцидент и др.), при настъпването на друго събитие (вследствие на отказ и др.) и е безразмерна величина в интервала от 0 до 1. По-точно рискът е свързан с отчитане на загубите, които неблагоприятното събитие може да донесе [А10]. Тогава малко вероятни събития, но с големи щети, могат да носят по-голям риск.

2.3. Дефиниране на основна структура и основни параметри на ИВУС

На фигура 2.1 е показана примерна структура на ИВУС (пирамида на ИВУС) с интегриран процес за управление на корпоративния риск, в която по отношение на основната структура и основните параметри на модела на ИВУС са използвани следните понятия и съкращения:

- Наблюдение и измерване – извършва се непрекъснато наблюдение и измерване на параметрите на ИВУС от старшия управленски състав. Това включва вътрешно одитиране, документиране на резултати, наблюдение и оценка на тяхното развитие, измерване на тяхната оперативна и финансова ефективност.
- Контролни механизми (добри практики) – съвкупност от организационни и технически контролни механизми (превантивни, детективни и коректривни), използващи приети добри практики.
- Управление на риска – модел за управление на цялостния корпоративен риск.
- Обхват – обхват на прилагане на отделните сфери в модела на ИВУС



Фиг. 2.1. Структура на ИВУС.

- 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.

Дефиниране на изисквания към модела на ИВУС

В тази глава се разработва модел на ИВУС въз основа на приети ограничителни условия, който включва основна структура, основни дефиниции и параметри на модела. Извежда се необходимото и достатъчно условие за създаване и внедряване на ИВУС в дадена информационна/телекомуникационна структура, под форма на регистър с изисквания и с механизми за контрол.

Ограничителни условия за модела

- 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 (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.

2.4. Същност на модела на ИВУС

Моделът на ИВУС е схема по която се разработва ИВУС в корпоративни структури и включва различни модули, което позволява непрекъснато разширение. Количеството на системите в ИВУС зависи от нуждите на съответната организация. Тя се състои от общи и от специфични модули, но може в допълнение да се включат и други изпитани и проверени системи за управление, съдържащи се в други области като например: управление на риска; управление на качеството; управление на околната среда; професионално управление на здравето и безопасността; управление на информационната сигурност; управление на извънредни ситуации; управление на изпълнителите и доставчиците; спазването на правни, договорни и други регулации.

Изискванията спрямо СУ (например сертификация на СУ за конкретен клиент), включване на нови сфери и др. специфични за сектора [А7], се определят от целите и основната дейност на организацията и заинтересованите (например клиенти, законодател и др.). Това означава, че за ИВУС, трябва да се формулират цели за контрол и механизми за контрол съгласно изискванията на приложимите технически стандарти, което да дава възможност за последващо сертифициране.

Придружаващият синергичен ефект в рамките на няколко области е една от основните причини за развитието на ИВУС в компанията. Тъй като системите за управление са подобни по структура и състав, интеграцията се случва с малко допълнителни усилия.

В таблица 2.2 е показан основният модел на ИВУС във вид на матрица, въз основа на която се изгражда интегрирането между различните СУ. Спазвайки логическата последователност на клаузите във всеки стандарт, са представени основните акценти, на които трябва да се обърне внимание по време на разработването на ИВУС. Тъй като стандартите са международни и сравнително уеднаквени като формат и структура, при въвеждането и изграждането на интеграция е препоръчително да бъдат „застъпени“ сходните и повтарящите се моменти в различните стандарти с цел избягване на усложняване и бюрократизиране на документацията.

Включените клаузи от международно приети стандарти са подбрани по сферите на ИВУС и които, следвайки модела за прилагане на ИВУС, третират областите му на приложение.

Алгоритъм за създаване на ИВУС

Алгоритъмът за създаване на ИВУС представлява процедура за интегриране на няколко СУ в ИСУ и може да се представи чрез фиг. 2.2.

2.5 Приноси към втора глава

От разработките във втора глава могат да бъдат направени следните **изводи**:

- Към момента не съществува единна и унифицирана методика за интеграция на различни системи за управление в цялостна интегрирана система.

Таблица 2.2. Модел на ИВУС

Изискване	Клауза от ISO 9001	Клауза от ISO 14001	Клауза от OHSAS 18001	Клауза от ISO 27001
Общи изисквания	4.1	4.1	4.1	4.3
Политика	5.3	4.2	4.2	5.2
Наръчник	5.3	4.4.4	4.4.4	5.2
Аспекти на околната среда	-	4.3.1	-	-
Идентифициране на опасности, оценка на риска от тях и определяне на контроли	-	-	4.3.1	6.2
Информационна сигурност	-	-	-	Анекс А
Правни изисквания	-	4.3.2	4.3.2	А.18
Цели, задачи и програми	5.4.1, 5.4.2	4.3.3	4.3.3	6.2
Ресурси, роли, отговорности, отчетност	5.5.1, 5.5.2, 6.1	4.4.1	4.4.1	5.1, 5.3, 7.1
Обучения, компетентност и осъзнатост	6.2.2	4.4.2	4.4.2	7.2, 7.3
Вътрешна и външна комуникация, комуникационни канали	5.5.3	4.4.3	4.4.3.1	7.4
Документация	4.2.1, 4.2.2	4.4.4	4.4.4	7.5
Управление на документите	4.2.3	4.4.5	4.4.5	7.5
Управление на записите	4.2.4	4.5.4	4.5.4	7.5
Оперативни контроли за дейността	-	4.4.6	4.4.6	8.1
Действия при бедствия и извънредни ситуации	-	4.4.7	4.4.7	А.11.1.4
Мониторинг и измерване на ефикасността	7.6, 8.2.3, 8.2.4	4.5.1	4.5.1	9.1
Съответствие	-	4.5.2	4.5.2	А.18.1
Действия при инциденти	-	-	4.5.3.1	А.16
Несъответствия, коригиращи и превантивни действия	8.5.2, 8.5.3	4.5.3	4.5.3.2	10.1
Вътрешен одит	8.2.2	4.5.5	4.5.5	9.2
Преглед от ръководството	5.6	4.6	4.6	9.3
Оперативен контрол на изпълнението	8.2.4	4.4.6	4.4.6	8.1

- Липсата на единна и унифицирана методика създава предпоставки за разработване на модел, който би могъл да бъде прилаган многократно от различни организации от телекомуникационния сектор, според контекста на настоящия труд.
- Моделът на ИВУС се разработва след взимане предвид на изискванията за разработката му и ограничителните условия.
- Направеният анализ и разработки представляват процес на оптимизиране на различните системи за управление и обосновка за създаването на интегрирана управленска система (ИВУС).

Приноси от втора глава:

2.1 Разработен е модел на ИВУС, въз основа на приети ограничителни условия.

2.2 Предложени са структура, дефиниции и параметри на модела на ИВУС.

2.3 Изведено е необходимото и достатъчно условие за създаване и внедряване на ИВУС в дадена телекомуникационна структура, под форма на регистър с изисквания и механизми за контрол.

2.4 Разработен е модел на ИВУС за управление на качеството, сигурността на информацията, сигурността по време на работата и на управлението на околната среда, според стандартите ISO 9001, ISO 27001, OHSAS 18001 и ISO 14001.

Публикации по втора глава: [A1], [A2], [A4], [A6], [A7], [A8], [A10].

Фиг. 2.2. Алгоритъм за създаване на ИВУС.

ГЛАВА 3. АНАЛИЗ НА УПРАВЛЕНИЕТО НА РИСКА С ИЗПОЛЗВАНЕ НА ИВУС

Процесът на оценка на риска, приложен последователно в цялата организация, дава възможност за по-добро управление, идентифициране, оценяване и третиране на рисковете за бизнеса. Това изисква внедряване и поддържане на необходимия контрол във всички сфери на бизнеса (процеси, качество, околна среда, сигурност, производство и др.), за да се гарантират качествени и ефективни операции с едновременно спазване на регулаторните изисквания.

3.1. Дефиниция и анализ на процеса „оценка на риска“

Оценката на риска е систематичен процес за идентифициране и оценка на събития (т.е. възможните рискове и заплахи), които биха могли да повлияят отрицателно на постигането на корпоративните цели. Такива събития (събитие е „идентифицирана поява на състояние в процес, услуга, система или мрежа, показваща възможно нарушаване на корпоративните оперативни правила (изисквания на интегрирана вътрешна управленска система (ИВУС), пробив на контролен механизъм или неизвестна до момента ситуация засягаща оперативната дейност)“) могат да бъдат идентифицирани в бизнес средата (например, икономически тенденции, регулаторните изисквания, конкуренцията и др.) и в рамките на вътрешно корпоративната среда (например, хора, процеси, инфраструктура и др.) на организацията.

Когато тези събития се пресичат с организационните цели, тогава възникват рискове. Затова рискът се дефинира като „възможността, че дадено събитие ще се случи и че ще възпрепятства постигането на целите до някаква степен”. Качествено разработеният и внедрен процес за управление на риска формира фундамента за корпоративно интегрирано управление на риска на ИВУС, което е и изискано от международно признат и прилаган стандарт COSO Enterprise Risk Management - Integrated Framework (Комитет на спонсориращите организации). Важно е да се разбере взаимовръзката между корпоративната оценка на риска, контролните механизми и наблюдението на ефективността. За илюстрация на гореописаното може да се използва моделът на ИВУС с интегриран процес за управление на корпоративния риск (фиг. 2.1).

Видове корпоративни активи

Предлага се разглеждането на 9 категории корпоративни активи като част от оценката на риска, описани в табл. 3.1. Процесът на определяне на активи е приведен в съответствие с изискванията за сигурността на ISO/IEC 27001:2013.

Описът на активите трябва да включва нужната информация подредена по значимост за бизнеса, включваща вида на актива. Списъкът не бива да е прекалено детайлен, но трябва да осигури подредбата на активите в тяхната изчерпателност. За всеки актив следва да е посочен собственикът, респективно държателят на риска му. Активите следва да се идентифицират и класифицират в зависимост от значимостта им, тяхната бизнес стойност, класификацията на сигурността и нивата на защита.

Видове влияещи събития при анализа на процеса „оценка на риска“

Събитията могат да бъдат категоризирани по различни начини. Например, те могат да бъдат обединени в една матрица, с хоризонтални редове посочващи категории рискови коренни причини и вертикални колони, представляващи процеси на бизнеса или функционални области. Всички приложими области на възникване на риск могат

съответно да се отбелязват. Друг подход се състои в улавяне на всички съответни видове събития и свързване на тези с по-широките категории, както е показано в табл. 3.2.

Табл. 3.1. Пример за видове активи на телекомуникационна структура.

ТИП АКТИВ	ПОЯСНЕНИЕ
Процеси	Състои се от набор от логически свързани индивидуални задачи (операции) с цел извършване и постигане на бизнес или оперативна цел.
Информации	Информации на логичен и хартиен носител.
Сгради и обекти	Сгради и физическа сградна инфраструктура.
Хардуер и софтуер	ИКТ – Решения, сървари, рутери, апликации и други
Доставчици	Критични и некритични трети страни - доставчици, които предоставят средства за поддържане на операциите на бизнеса, на мрежите, системите, услугите или продуктите на компанията.
Клиенти, решения и продукти	Данни за клиента и документация за консумирани услуги и продукти (решения), статистически данни и др.
Човешки ресурси	Човешки ресурси на компанията.
Immaterielle Werte	Сертификати, лицензи и други.

Табл. 3.2. Пример (съкратен) за категоризиране от гледна точка на външни и вътрешни събития.

Събития	Групи	Източник			
Външни	Икономически	Разпад на финансови пазари	Безработица	Сливания и придобивания	Конкуренция
Вътрешни	Инфраструктура	Наличност на активи	Способност на активите	Достъп до активите	Сложност на активите

Типове оценки на риска в интегрирана система за оценка на риска

Оценката на риска може да се проведе на различни нива (топ мениджмънт, среден мениджмънт и др.) и сфери (управление на качеството, доставяне на услуги и др.) на организацията. Целите и събитията, които се обсъждат, определят обхвата на оценката на риска, както и дейности, които трябва да бъдат предприети след анализ на неприемливия риск. Разгледани са различни примери за често извършвани оценки на риска.

Особености на корпоративната оценка на риска

За да бъде ефективна, оценката на риска не може да бъде просто един списък или процес, който е изключен от процеса на вземане на бизнес решения. Вместо това, тя трябва да бъде интегрирана в управленския бизнес процес и сферите му, по начин, който да осигурява навременна и актуална информация за рисковете и тяхното управление. Оценката на риска, трябва да бъде един непрекъснат процес, той трябва да бъде управляван от бизнеса и да се вгражда в рамките на работния цикъл, като се започне със стратегическо планиране, осъществявано чрез бизнес процесите и завършва с оценка, както е показано в табл. 3.3.

Таблица 3.3. Бизнес цикъл на примерна телекомуникационна компания.

	ФАЗА 1 – СТРАТЕГИЯ	ФАЗА 2 – ПРОЦЕСИ И ИЗПЪЛНЕНИЕ	ФАЗА 3 – ОЦЕНКА НА РИСКА
Ключови фази на бизнес цикъл	Бизнес стратегия и планиране	Бизнес процеси и тяхното изпълнение	Оценка
Ключови контролни	Организационни контролни	Организационни и	Докладване на анализ на

механизми	механизми	технически контролни механизми	риска в различните оперативни функции
Оценка на риска	Изрично интегриране на риска в стратегическите планове Определяне „апетита" към риск и да се осигури неговата съгласуваност със стратегията Разпределяне на икономическия капитал по бизнес единици/рискови дейности Определяне на бизнес и индивидуални цели за изпълнение	Изрично интегриране на риска в стратегическите планове Определяне на склонността към риск и да се осигури нейната съвместимост със стратегията Разпределение на икономическия капитал по бизнес единици/предприятия Идентифициране на бизнес и индивидуални цели за изпълнение	Доклад с резултати и препоръки.

3.2. Дефиниране на критерии за анализ на риска

Метриката за измерване на риска се базира на вероятност и въздействие, както е показано в таблица 3.4.

Таблица 3.4 Критерии за анализ на риска, спрямо вероятността (горните редове) и спрямо въздействието (долните редове).

Вероятност	**Дефиниции**	**Описание**	**Пример**
1	Много ниско	Рискът се разглежда като малко вероятно да се случи в рамките на времевия хоризонт (например 1 година).	Мерки за физическа сигурност като например видео наблюдение, охрана, картова система са внедрени, но въпреки това има вероятност да има физически пробив.
2	Ниско	Рискът се разглежда като вероятност да се случи в рамките на времевия хоризонт (например 1 година).	Пример по горе.
3	Средно	Рискът е по-вероятно да се случи в рамките на времевия хоризонт.	Картовата система на компанията работи без съществено криптиране на картовата информация (права за достъп). Възможно е копиране на карта за достъп.
4	Високо	Рискът е вероятно да се случи в рамките на времевия хоризонт, до 1 месец.	Пример по горе.
5	Много Високо	Рискът се очаква да се случи в рамките на времевия хоризонт, всеки момент.	Физическата охрана не е обучена адекватно, което ще доведе до инцидент в сферата на физическата сигурност.
Въздействие	**Дефиниции**	**Описание**	**Пример**
1	Много ниско	Рискът ще нанесе минимални щети (до например 10000 евро) на активи на организацията.	Отпадане на поддържаща некритична система. Оперативната дейност не е застрашена.
2	Ниско	Рискът ще нанесе минимални щети (до например 30000 евро) на	Отпадане на поддържаща некритична система. Оперативната дейност не е застрашена.

Вероятност	Дефиниции	Описание	Пример
		активи на организацията.	
3	Средно	Рискът ще нанесе умерени щети на активи на организацията.	Отпадане на оперативно важна поддържаща система. Оперативната дейност е застрашена, но все още е активна.
4	Високо	Рискът ще нанесе съществени щети (до например 1 милион евро) на активи на организацията.	Отпадане на оперативно важна поддържаща система. Оперативната дейност е застрашена, но все още е активна.
5	Много Високи	Рискът ще нанесе критични щети на активи на организацията. Отпадане на най-критичните услуги.	Отпадане на оперативно важна критична за дейността система. Оперативната дейност е застрашена и отпада.

Измерването на риска спрямо определените критерии и параметри на реакция, са посочени в таблица 3.5.

Рискът следва да бъде управляван, вземайки предвид параметрите вероятност за случване на събитие и въздействие от събитието. За целите на настоящата работа е представен модел с пет степени на вероятност и въздействие – много ниско, ниско, средно, високо, много високо.

Таблица 3.5 Модел за оценка на риска и управлението му

Въздействие						
	Много високо					Третирай риска
	Високо					
	Средно			Предай риска или сподели риска		
	Ниско					
	Много ниско	Приеми риска				
		Много ниско	Ниско	Средно	Високо	Много високо
		Вероятност				

Когато събитията попадат в ниско или много ниско ниво на вероятност и въздействие, тогава те биха могли да бъдат приети във вида, в който са след извършване на анализ за цената, която следва да бъде платена за третиращи (минимизиращи) рисковете контроли и преценка дали тези разходи са оправдани.

Когато събитията попадат в средните нива на вероятност и въздействие, тогава рискът следва да бъде третиран (трансфериран или минимизиран), отново след задълбочен анализ на разходите спрямо ползи.

Когато рисковете са с високи или много високи стойности на вероятност и въздействие, тогава е силно препоръчително да бъдат въведени третиращи (минимизиращи) риска контроли с цел запазване на целостта на бизнес процесите.

3.3. Анализ на оценката на риска в ИВУС

Провеждат се следните стъпки на оценката на риска в ИВУС:

1. Дефиниране на нивото на оценката на риска в ИВУС (топ мениджмънт, среден мениджмънт и др.);
2. Дефиниране на сфери (управление на качеството, доставяне на услуги и др.) на организацията;
3. Целите и събитията, които се обсъждат, определят обхвата на оценката на риска, както и дейности, които трябва да бъдат предприети след анализ на неприемливия риск.

3.4. Модел и алгоритъм за оценка на корпоративния риск като част от ИВУС

Основни стъпки за извършване на оценка на риска

Извършването на оценка на риска изисква текущо и последователно прилагане на метод/подход, който е съобразен с организацията. Всяка проведена оценка на риска трябва да започне със създаването на обхват и план, имайки предвид целите, отговорностите, времето, както и входните и изходните изисквания. Отговорности в процеса на оценка на риска са възложени на пряко свързани служители, които могат да дадат смислен поглед върху съответните рискове.

Източници на входни данни се определят въз основа на наличната информация (например, предварителни оценки, загуба на данни, извлечените поуки).

Изходната информация на процеса се планира въз основа на спецификациите в изискванията на спонсори и други заинтересовани страни (например, висш ръководен състав, на борда, регулатори, акционери или бизнес партньори).

След като определянето на обхвата и планирането са извършени, изпълнението на процеса на оценка на риска трябва да включва следните основни стъпки: Идентифициране на процеси и активи, както и рискове; Идентифициране на събитие; Определение на критерии и изисквания спрямо оперативната дейност и нейните рискове; Оценка на риска; Реакция спрямо риска (приемане на риск, прехвърляне на риск, третиране на риск).

Тези основни стъпки са илюстрирани на фиг. 3.1.

3.5. Примерни контролни механизми за третиране (снижаване) на риска, прилагани в ИВУС

Разгледани са примерни контролни механизми за снижаване на риска, прилагани в ИВУС, например: политика по информационна сигурност, физическа сигурност на информацията и др., посочени в дисертацията.

Фиг. 3.1. Алгоритъм за оценка на корпоративния риск като част от ИВУС.

3.6. Основни принципи за ефективно прилагане на модел за оценка и за управление на риска

За да се получават смислени и ценни резултати от процеса за оценка и управление на риска, е нужно спазването на минимални изисквания спрямо прилагането на модела в оперативната корпоративна среда.

Управлението на процеса за оценка на риска, трябва да бъде ясно дефинирано и документирано. Надзорът и отчетността на процеса на оценка на риска е от решаващо значение, за да има гаранция, че необходимите ресурси са обезпечени. Процесът на оценката на риска трябва да бъде внедрен в управленското ниво на организацията и трябва да бъде поддържан пряко от това ниво, за да може да се счита, че рискове се оценяват чрез строго регулиран и непрекъснат процес и че необходимите корективни действия са възможни и могат да бъдат предприети.

Изисква се от организацията дефиниране на цели, които са конкретни и измерими и покриват различните нива на организацията. Оценка на рисковете по отношение на тези цели улеснява преразпределението на ресурсите, необходими за управление на тези рискове и най-доброто постигане на поставените цели.

Рисковият рейтинг, трябва да бъде определен в количествено и/или качествено отношение. Рисковете обикновено се измерват по отношение на тяхното въздействие и вероятността им за настъпване. Времевият хоризонт, използван за оценка на вероятността за риск, следва да бъде в съответствие с времевите хоризонти, свързани с целите.

Количествените рейтингови скали позволяват по-голяма степен на точност и измеримост на процеса на оценка на риска. Въпреки това, те се нуждаят от качествена гледна точка, която да може да се използва, когато рисковете не се поддават на количествено определяне, когато достоверни данни не са на разположение или когато получаването и анализирането на данни не е икономически ефективно.

Организациите обикновено използват следните мащаби за измерване на риска: редни, интервални и/или съотносителни. Редните мащаби определят ранга, реда на важност (например, ниска, средна или висока), интервалните мащаби имат числено разстояние (например, най-ниското е равно на 1, а най-високото е равно на 3, но при това най-високото не е 3 пъти по голямо от най-ниското), а съотносителните мащаби дават възможност за по-голяма измеримост (например, класиране на 10 нива е 5 пъти по-голямо от класиране на 2). Описаните типове измерителни мащаби не са приложими за всяка компания без тяхното конкретизиране.

3.7 Приноси към трета глава

В трета глава могат да бъдат направени следните **изводи**:

- Оценката на корпоративния риск трябва да бъде интегрирана в управленския бизнес процес и сферите му, по начин, който да осигурява навременна и актуална информация за рисковете и тяхното управление.
- Оценката на риска, трябва да бъде един непрекъснат процес, той трябва да бъде управляван от бизнеса и да се вгражда в рамките на работния цикъл, веднага когато се започне със стратегическо планиране, осъществявано чрез бизнес процесите и завършва с оценка, както е показано.
- Оценката на риска трябва да се задейства в рамките на работния процес, когато възникват особени обстоятелства извън текущия бизнес цикъл,
- Преди вземане на решение за въвеждане на нов контрол, е препоръчително да бъде измерено до каква степен контролираното събитие би могло да се случи и какво би било въздействието след случването му.

Приноси от трета глава:

3.1. Представен е разработен модел за управление на корпоративния риск като част от ИВУС.

Публикации по трета глава: [A3], [A10].

ГЛАВА 4. ОПЕРАТИВНА ЕФЕКТИВНОСТ НА ИВУС

4.1. Модел 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 (Eiks).

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

Ni =0 **Ekg=К1** (в случай, че няма установени инциденти);

Ni≠0 tdi≤td and tfi≤tf **Ekg=К2** (в случай, че превантивните контролни механизми не са сработили, но детективните и коректривните контролни механизми са сработили (в определените им времена за реакция));

Ni≠0 tdi>td and tfi≤tf **Ekg=К3** (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);

Ni≠0 tfi>tf **Ekg=К4** (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:

Eiks	- Ефективност на системата за вътрешен контрол,
Kg	- Контролна група / задача група,
Ni	- Инциденти по сигурността,
Td	- Дефинирано време за откриване на инцидента,
Tf	- Дефинирано време за премахване на инцидент,
Tdi	- Време на възникване на инцидента по сигурността,
Tfi	- Реално време за премахване на инцидент по информационна сигурност.

Ограничителни условия:

1. Авторът приема четири случая и съответно приема четири константи като гранични стойности.

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

Тези ограничителни условия се базират на постановката, описана в ISO/IEC 27004:2009, че нивото на гранулираност и съответното детайлизиране на оценката на ефективността се определя от компанията, прилагаща такъв модел. Определя се 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.

Примерни рамки за категоризиране

ИВУС изисква индивидуален анализ на корпоративните структури и техните оперативни дейности [A10]. 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").

Типове инциденти

Категоризацията на типовете инциденти спрямо щетите от въздействието на заплаха върху операциите в съответна компания е показана в таблица 4.1.

Таблица 4.1 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 таблица 4.2.

Таблица 4.2 Категоризация на изискванията за времената на реакция на контролните механизми.

Тип инцидент	**Тип контрол**	**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

С илюстративна цел са създадени четири броя контролни групи (таблица 4.3[2]), които включват вид на риска, контроли, които следва да бъдат въведени (превантивен, детективен и коригиращ), както и наименованието на контролната група за целите на модела.

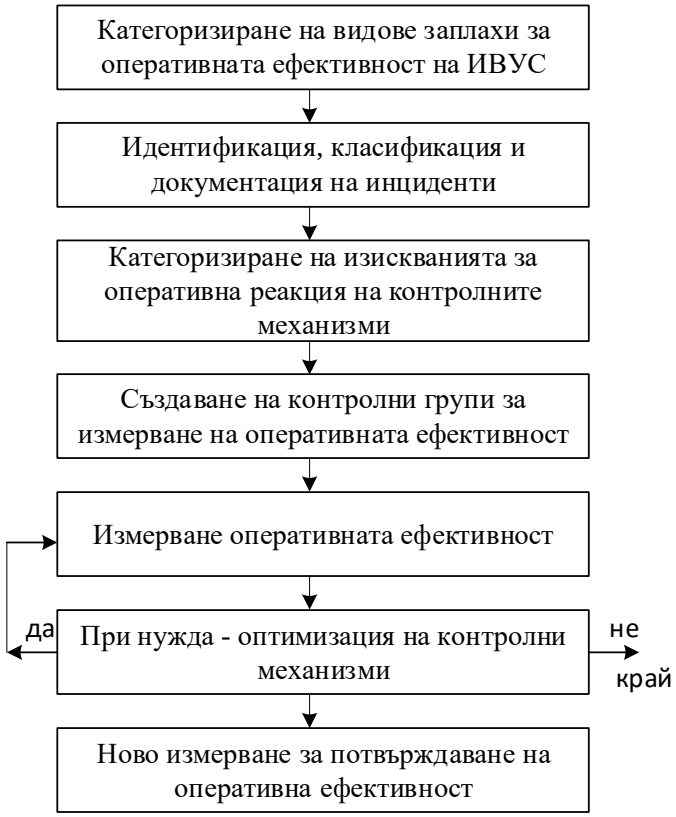
4.2. Алгоритъм за оценка на оперативната ефективност на ИВУС

На база на анализа на функциониране на модела на ИВУС, може да се предложи разработен алгоритъм за оценка на нейната оперативна ефективност [A9], показан на фиг. 4.1.

[2] Съкратена примерна таблица. Пълното съдържание се съдържа в дисертацията.

Таблица 4.3. Категоризация на изисквания за реакция на контролните механизми.

Риск	Контрол	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	



Фиг. 4.1. Алгоритъм за оценка на оперативната ефективност на ИВУС.

4.3. Приноси към четвърта глава

В четвърта глава, могат да бъдат направени следните **изводи**:

- Всяка ИВУС следва да разполага с разработен аналитичен модел и алгоритъм за оценка на оперативната ефективност.
- За коректното функциониране на модела следва да бъдат разработени контролни групи, които съдържат определени контролни механизми, всеки от които е в съответствие с типа на контролата (превантивна, детективна и коригираща).

- Оперативната ефективност на ИВУС следва да се определя от средната стойност на ефективността на контролните групи.
- ИВУС изисква индивидуален анализ на корпоративните структури и техните оперативни дейности. Чрез анализа следва да се дефинират константи и дефиниции за типовете инциденти, контролните изисквания спрямо управленската система и създаването на контролни групи.

Приноси от четвърта глава:

4.1. Синтезиран е алгоритъм за измерване на оперативната ефекивност на ИВУС.

4.2. Дадени са контролните изисквания за прилагане на алгоритъма за измерване на оперативната ефекивност на ИВУС. Представени са примери за прилагане на алгоритъма.

4.3. Определени са типовете контроли и измерителите за ефективност на всеки от контролите, въз основа на примерни инциденти.

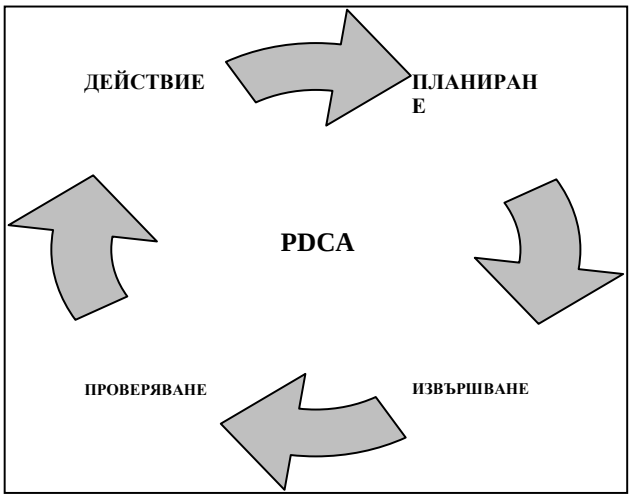
Публикации по четвърта глава: [A9], [A10].

ГЛАВА 5. МЕТОДИКИ И АЛГОРИТМИ ЗА ИЗПОЛЗВАНЕ НА МОДЕЛА НА ИВУС

В настоящата глава са показани обосновани методики и алгоритми за използване на модела на ИВУС в съответствие с практиката за управление (т. 5.1).

5.1. Стратегия за непрекъснато подобрение

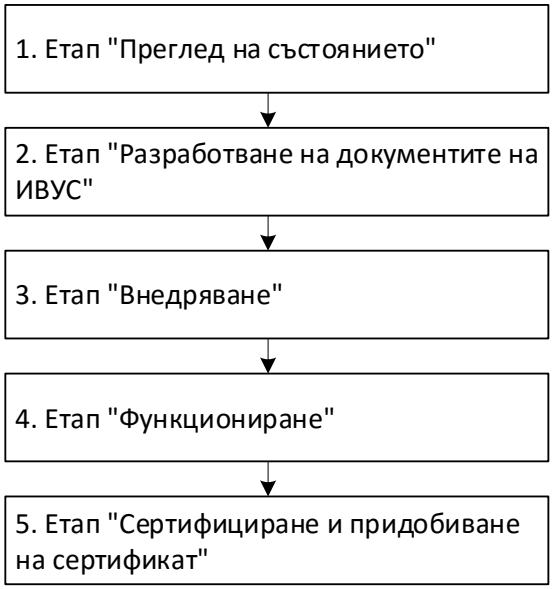
Вътрешните контролни системи интегрирани като част от разработената ИВУС в този дисертационен труд [А5], се базират на международно приетата стратегия за непрекъснато подобрение според цикъла на Деминг (фиг. 5.1).



Фиг. 5.1. Цикъл на Деминг – PDCA.

5.2. Етапи и алгоритъм на внедряване с използване на ИВУС

Процесът по разработване и внедряване на ИВУС е илюстриран на фиг. 5.2, като е представена и разбивка на етапите с основните моменти, които включва всеки един от тях.



Фиг. 5.2. Етапи и алгоритъм на внедряване с използване на ИВУС.

5.3. Особености при използването на ИВУС

Въвеждането на ИВУС позволява на организациите да решат следните проблеми, които често възникват при паралелно или последователно независимо внедряване на няколко СУ според международни стандарти, например разпокъсване на взаимовръзките между системите за управление на качеството, околната среда, здравето и безопасността при работа и т.н. по време на независимото внедряване, и др. (пълното съдържание се съдържа в дисертацията).

Моделът на ИВУС, разработен в настоящата работа за организации предимно в телекомуникационния сектор, е структуриран и изграден с крайна цел минимизиране или напълно отстраняване на част или на всички от изброените по-горе проблеми, които често присъстват при организациите, опитващи се да се сертифицират по различни стандарти чрез отделни системи или използвайки неефективни методи за интеграция между различните стандарти. Моделът на ИВУС използва основните моменти във всеки стандарт, т.нар. „клаузи за съответствие" и ги съпоставя и сравнява с други клаузи със същата или подобна тематика. **Това е основна приложна ценност на разработения модел.**

Разработеният модел на ИВУС, както и конкретна структура на ИВУС следва да бъдат адекватно внедрени в организацията. Това може да бъде извършено след обстоен анализ на обстановката, работната среда, функциониращите процеси и комуникационни канали. Чрез иползването на световно наложени методи за непрекъснато подобрение и контрол, ИВУС се разработва и внедрява по ефективен път, без да натоварва бизнес дейностите.

5.4. Приноси към пета глава

В пета глава, могат да бъдат направени следните **изводи**:

- Използването на процеси, гарантиращи непрекъснато подобрение, води до значителни измерими ползи в дългосрочен план.
- Изграждането на ИВУС следва да бъде извършено при спазване на предварително разработен и впоследствие одобрен план за разработката, включващ различни етапи.

Приноси от пета глава:

5.1. Описани са основните ползи при интеграция на стандартите в единна система при използване на модела на ИВУС.

5.2. Предложен е метод за внедряване на модела на ИВУС, като са представени основните пет етапа, базирани на цикъла на Деминг, при реализация на цялостно решение по разработване и внедряване на ИВУС.

Публикации по пета глава: [A5].

III. ЗАКЛЮЧЕНИЕ И ОСНОВНИ ПРИНОСИ

В настоящата дисертация, посветена на неизследваните въпроси за анализа и възможното оптимизиране на самостоятелно съществуващите вътрешни контролни системи в телекомуникационни структури, е изведена необходимостта от създаване на ИВУС. Понятието ИВУС се свързва със система за управление, интегрираща приети компоненти с помощта на специфично изготвен модел на базата на дефинирана структура. Целта на използването на модела на ИВУС е унифициране и стандартизиране на процеса по интеграция с оглед на повишаване на ефективността и ефикасността, което води до неговото оптимизиране. Изграждането на ИВУС създава една цялостна прозрачна система включваща ясни логически връзки, гарантираща управляема ефикасност и оптимална функционалност на процесите.

Необходимостта от създаване на ИВУС е продиктувана от наблюденията на автора, че към момента не съществува единна и унифицирана методика за интеграция на различни системи за управление в цялостна интегрирана система. Липсата на единна и унифицирана методика създава предпоставки за разработване на модел, който би могъл да бъде прилаган многократно от различни организации от телекомуникационния сектор, според контекста на настоящия труд.

Важна част от изграждането на ИВУС е функционирането на адекватна оценка на корпоративния риск. Тя трябва да бъде интегрирана в управленския бизнес процес и сферите му, по начин, който да осигурява навременна и актуална информация за рисковете и тяхното управление. Оценката на риска, трябва да бъде един непрекъснат процес, той трябва да бъде управляван от бизнеса и да се вгражда в рамките на работния цикъл, веднага когато се започне със стратегическо планиране, осъществявано чрез бизнес процесите и завършва с оценка, както е показано. Оценката на риска трябва да се задейства в рамките на работния процес, когато възникват особени обстоятелства извън текущия бизнес цикъл. Преди вземане на решение за въвеждане на нов контрол, препоръчително е да бъде измерен до каква степен контролираното събитие би могло да се случи и какво би било въздействието след случването му.

Всяка ИВУС следва да разполага с разработен аналитичен модел и алгоритъм за оценка на оперативната ефективност. За коректното функциониране на модела следва да бъдат разработени контролни групи, които съдържат определени контролни механизми, всеки от които е в съответствие с типа на контролата (превантивна, детективна и коригираща). Оперативната ефективност на ИВУС следва да се определя от средната стойност на ефективността на контролните групи. ИВУС изисква индивидуален анализ на корпоративните структури и техните оперативни дейности. Чрез анализа следва да се дефинират константи и дефиниции за типовете инциденти, контролните изисквания спрямо управленската система и създаването на контролни групи.

Разработването и внедряването на ИВУС е сложен, но управляем процес. Чрез прецизно планиране на време и ресурси, както и чрез спазване на основни принципи при разработването на ИВУС (етапи на изпълнение), системата придобива завършен вид и резултатите от нейното функциониране се показват скоро след финалната имплементация/внедряване.

Представеният модел и структура на ИВУС за телекомуникационни структури могат да бъдат широко приложими и в други сфери на дейност на организациите. Моделът на ИВУС е гъвкъв и позволява извършването на адекватна оценка на оперативната ефективност на системата, спрямо изискванията към нея и вложените в нея инвестиции.

Моделът на ИВУС е използван в разработката и внедряването на системи в различни организации в частния сектор, както и в структури в публичния сектор.

Като една възможност за продължение на тази разработка може да се предложи приложението на алгоритъма и доказване на ефективността в реални условия. В практиката на изследване, анализ и одитиране на ИВУС се използват много практически подходи, базирани на съответните стандарти.

Използването на структурата и модела на ИВУС биха могли да бъдат приложени и при интеграция на стандарти, различни от споменатите в настоящата работа. Разработващият системата екип следва да разполага със задълбочени познания относно структурите и изискванията на всеки стандарт и използвайки модела на ИВУС, да подходи по сходен начин в същинската интеграционна част.

В заключение може да се обобщи, че тематиката на дисертацията е актуална и дефинираните в първа глава цели са постигнати, като са получени следните **приноси**:

1. Направен е критичен анализ на въпросите свързани с управленски системи въз основа на разгледаната литература.

2. Разработен е модел на ИВУС, въз основа на приети ограничителни условия и са предложени структура, дефиниции и параметри на модела на ИВУС.

3. Предложен е модел и алгоритъм за управление на риска като част от ИВУС.

4. Синтезиран е модел и алгоритъм за измерване на оперативната ефективност на ИВУС и са дадени контролните изисквания за прилагане на алгоритъма, както и примери за прилагането му.

5. Определени са типовете контроли и измерителите за ефективност на всеки от контролите, въз основа на примерни инциденти.

6. Описани са основните ползи при интеграция на стандартите в единна система при използване на модела на ИВУС.

7. Предложен е метод за внедряване на модела на ИВУС, като са представени основните пет етапа, базирани на цикъла на Деминг, при реализация на цялостно решение по разработване и внедряване на ИВУС.

IV. СПИСЪК С ПУБЛИКАЦИИ ПО ТЕМАТА НА ДИСЕРТАЦИЯТА

Публикации във връзка с дисертацията:

[A1] Tomov K., B. Balabanov Analysis of the possibilities for combinations of strategies for information security management in ICT companies. In Proceedings of the „20th Annual International Conference Telecom 2012“, 18-19.10.2012, Sofia, pp. 22-32, ISSN: 1314-2690 (In Bulgarian: Анализ на възможностите за комбиниране на стратегии за управление на информационната сигурност на ИКТ фирми).

[A2] Tomov K., B. Balabanov Methodology for the information security management in an e-government environment. In Proceedings of the „International Telecommunication Union Regional Forum on Cybersecurity for Europe and CIS”, 23-26.10.2012, Sofia, (In Bulgarian: Методология за управление на информационната сигурност за средата на е-правителство), http://www.itu.int/ITU-D/eur/rf/cybersecurity/presentations/eGovernance%20security%20framework%20strategy-BB-Kristian.pdf.

[A3] Томов К., Б. Балабанов Рискове и отговорности при ИТ аутсорсинг. Конференция на „Българска Асоциация Телекомуникации (АСТЕЛ)“, 17.04.2013, София, http://www.astel-bg.com/bg/present_14.htm.

[A4] Tomov K. Analysis of internal control systems in telecommunication structures. In Proceedings of the „21th Annual International Conference Telecom 2013“, 17-18.10.2013, Sofia, pp. 188-198, ISSN: 1314-2690 (In Bulgarian: Анализ на вътрешни контролни системи в телекомуникационни структури).

[A5] Tomov K. Analysis of the national information security standard IT-Grundschutz and opportunities for implementation and certification. In Proceedings of the „21th Annual International Conference Telecom 2013“, 17-18.10.2013, Sofia, pp. 155-163, ISSN: 1314-2690 (In Bulgarian: Анализ на национален стандарт по информационна сигурност „IT-GRUNDSCHUTZ“ и възможности за внедрение и сертификация).

[A6] Tomov K. Integrierte Management Systeme, 22.05.2014 (http://www.all-about-security.de), http://www.all-about-security.de/security-artikel/organisation/security-management/artikel/16149-der-integrierte-managementsystemansatz/

[A7] Tomov K. Auswirkungen der Änderungen von ISO 27001:2005 zu ISO 27001:2013. 30.07.2014, (http://www.all-about-security.de), http://www.all-about-security.de/security-artikel/organisation/security-management/artikel/16283-auswirkungen-der-aenderungen-von-iso-270012005-zu-iso-27001/

[A8] Tomov K. Criteria for business continuity management systems in telecommunication structures. Annual Proceedings of New Bulgarian University (Department of Telecommunications), 2014, vol. 1, pp.151-160, ISSN 2367-5039 (In Bulgarian: Критерий на система за управление на непрекъсваемостта на бизнеса в телекомуникационните структури).

[A9] Tomov K. Development of an integrated internal management system (IICS) model and a efficiency measurement algorithm. Annual Proceedings of New Bulgarian University (Department of Telecommunications), 2014, vol. 1, pp. 161-167, ISSN 2367-5039 (In Bulgarian:

Разработка на модел на интегрирана вътрешна управленска система (ИВУС) и алгоритъм за оценка на оперативната ефективност).

[A10] Tomov K. Analysis of a risk assessment approaches and the development of an integrated internal management system risk assessment model. Annual Proceedings of New Bulgarian University (Department of Telecommunications), 2014, vol. 1, pp. 168-177, ISSN 2367-5039 (In Bulgarian: Анализ на подходи за оценка на риска и разработка на модел за оценка на риска за интегрирана вътрешна управленска система).

Забелязани ЦИТИРАНИЯ на научни публикации на маг. инж. Кристиан Томов

1. Petrov G., A. Stancheva, V. Kadrev Specialized databases for spectrum management research, analysis and forecasting of the effects of working electromagnetic fields. Annual Proceedings of New Bulgarian University (Department of Telecommunications), 2014, vol. 1, pp.118 - 126, ISSN 2367-5039.

[A2] **Kristian Tomov**, B. Balabanov, Frame/Methodology for the Information Security Management in an e-Government Environment, ITU Regional Forum on Cybersecurity for Europe and CIS, 23-25 October 2012, Sofia, Bulgaria

V. СПИСЪК И ДОКАЗАТЕЛСТВА ЗА ВНЕДРЯВАНИЯ И ИЗПОЛЗВАНИЯ НА РЕЗУЛТАТИТЕ на дисертационния труд на маг. инж. Кристиан Димитров Томов "АНАЛИЗ И ОПТИМИЗИРАНЕ НА ВЪТРЕШНИ КОНТРОЛНИ СИСТЕМИ В ТЕЛЕКОМУНИКАЦИОННИ СТРУКТУРИ" (референции и препоръки)

По тематиката на дисертационния труд е работено в рамките на проекти, изброено в препоръките от следните фирми:

1. Препоръка от ИД на „Информационно обслужване АД”
2. Препоръка от р-л „Вътрешен одит” на „Информационно обслужване АД”
3. Препоръка от ИД на „СУИС ЕООД”
4. Препоръка от АД на „БДЖ АД”
5. Препоръка от DPO на „Altran GmbH & Co KG”
6. Препоръка от DHG на „Interoute Germany GmbH”
7. Препоръка от IT-Security and Quality Manager на „Telehouse Deutschland GmbH”
8. Препоръка от IT-Security and Quality Manager на „KDDI Deutschland GmbH”
9. Препоръка от ISO на „VSE Verteilnetz GmbH”
10. Препоръка от Leiter RZ Betrieb на „IVZ GmbH”

Препоръките са приложени в дисертацията. Следва извадка.

information services plc

2, P. Volov Str.,
1504 Sofia, Bulgaria
tel: +359 2/ 942 03 40
fax: +359 2/ 943 66 07
e-mail: office@is-bg.net

SOFIA ID: 831641791 ISO 9001:2008, ISO/IEC 27001:2005 Certified www.is-bg.net

До всички заинтересовани!

Имам удоволствието да препоръчам г-н Кристиан Томов, който от 2009 г. до момента е част от екипа на „Информационно обслужване“ АД.

Организацията е една от водещите ИТ компании в България и предлага високотехнологични решения в областта на системната интеграция, изграждане и поддръжка на национални бази данни и електронни регистри, софтуерни продукти и електронен подпис, асемблиране и поддръжка на хардуерни системи. Предоставя консултантски услуги в областта на хардуера, софтуера и информационните технологии.

Г-н Томов участва активно в процеса на планиране, внедряване и поддържане на Системата за управление на сигурността на информацията, съгласно изискванията на международния стандарт ISO/IEC 27001:2005. В този важен за Дружеството период г-н Томов прояви изключително чувство за отговорност, способност за поемане на натоварване и самообладание в извънредни ситуации.

В качеството си на “Information Security & Risk manager”, г-н Томов изготви цялостното ИТ управление на риска; прилагане, наблюдение и измерване на вътрешни контроли за управление на риска; докладване, управление и анализ на инциденти по ИС; обучение на служителите по ИС; изготвяне и актуализиране на документацията по информационна сигурност; проверка на изпълнението на коригиращи действия по информационна сигурност.

Като одитор по информационна сигурност, г-н Томов провежда Вътрешните одити на Интегрираната система за управление на качеството и информационната сигурност в организацията, спрямо ISO/IEC 27001:2005 и ISO 9001:2008.

В изпълнение на служебните задължения се отнася с изключителна професионална компетентност и обективност, целенасоченост при преследването на поставените цели. Благодарение на инициативността си г-н Томов е в помощ и подкрепа на служителите от отделните структурни единици, и по време на вътрешните одити работи целеустремено за просперитета на Дружеството. Оказва постоянна професионална подкрепа на своите колеги. През време на работата си за „Информационно обслужване“ АД г-н Томов повишава квалификацията си и проявява гъвкавост при поставяне на нови задачи.

Като член на нашия екип г-н Томов доказа на практика своята професионална компетентност в областта на ИТ технологиите и информационната сигурност.

С уважение,

Чавдар Тодоров
Изпълнителен директор
„Информационно обслужване“ АД

КОМПЕТЕНЦИИ НА МАГ. ИНЖ. КРИСТИАН ТОМОВ ПО ТЕМАТА НА ДИСЕРТАЦИЯТА

1. Сертификат за вътрешен одитор по следните управленски стандарти: ISO 9001, ISO 14001, OHSAS 18001.

2. Сертификат за водещ одитор по информационна сигурност ISO 27001.

3. Сертификат за водещ обучител по информационна сигурност ISO 27001 и др.

MOODY INTERNATIONAL

CERTIFICATE

Moody International EOOD certifies that

Kristian Tomov

Has attended a three-day course and successfully passed an examination as

INTERNAL AUDITOR

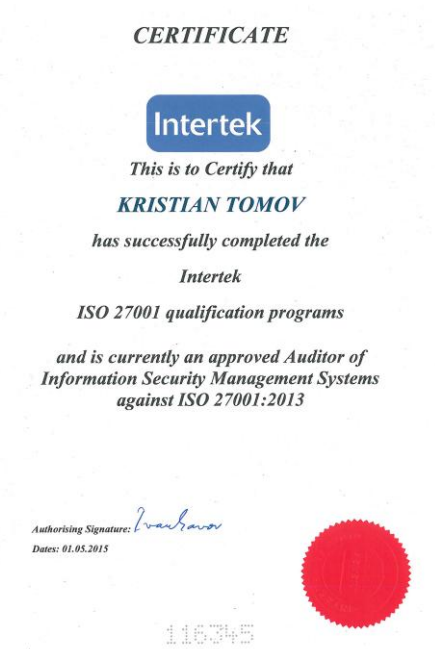
OF INTEGRATED MANAGEMENT SYSTEMS

ISO 9001:2008, ISO 14001:2004, OHSAS 18001:2007

Course № IA IMS BG 09-10

Date: 9 - 11 September 2009

Authorized signature:



CERTIFICATE

Intertek

This is to Certify that

KRISTIAN TOMOV

has successfully completed the

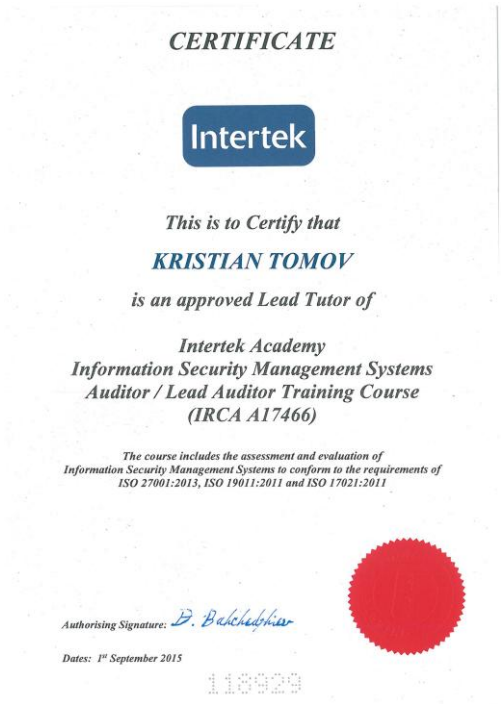
Intertek

ISO 27001 qualification programs

and is currently an approved Auditor of Information Security Management Systems against ISO 27001:2013

Authorising Signature:

Dates: 01.05.2015



CERTIFICATE

Intertek

This is to Certify that

KRISTIAN TOMOV

is an approved Lead Tutor of

Intertek Academy
Information Security Management Systems
Auditor / Lead Auditor Training Course
(IRCA A17466)

The course includes the assessment and evaluation of Information Security Management Systems to conform to the requirements of ISO 27001:2013, ISO 19011:2011 and ISO 17021:2011

Authorising Signature:

Dates: 1st September 2015