

ГЛОБАЛНИ ПЕРСПЕКТИВИ ЗА РАЗВИТИЕТО НА ПРОФЕСИЯТА ВЪТРЕШЕН ОДИТОР

год. XXIII, брой 2/2026 www.iiabg.org



**GLOBAL
ASSEMBLY**
Where it all Comes Together.

**THE ONE IIA – ЗАЕДНО ГРАДИМ
БЪДЕЩЕТО НА ВЪТРЕШНИЯ ОДИТ**

**ВЪТРЕШНИЯТ ОДИТ
ПРАВИ КРАЧКА НАПРЕД**

**МОЖЕ ЛИ ЕДИН МАЛЪК ОДИТЕН ЕКИП
ДА ПОКРИЕ ГОЛЯМА ОДИТНА ВСЕЛЕНА?**



Certified for Success.

Success is measured by
the impact you make.



The Institute of
Internal Auditors
Elevating Impact



ВЪТРЕШЕН ОДИТОР

специализирано списание на
Института на вътрешните одитори в България

ГОДИНА XXIII | брой 2 | 2026



СЪДЪРЖАНИЕ

2 СТРАНИЦАТА НА ГЛАВНИЯ РЕДАКТОР

4 НОВИНИ ОТ ИВОБ

THE ONE IIA – ЗАЕДНО ГРАДИМ БЪДЕЩЕТО НА ВЪТРЕШНИЯ ОДИТ

Цветан Цветков и Димитър Нешев

10 ВЪТРЕШНИЯТ ОДИТ ПРАВИ КРАЧКА НАПРЕД

Anthony Pugliese

Превод: Светлана Иванова

18 ИЗИСКВАНИЯТА НА IIA ЗА ОДИТ НА КИБЕРСИГУРНОСТТА – ПРАКТИЧЕСКИ НАСОКИ ЗА ВЪТРЕШНИТЕ ОДИТОРИ

24 ОТ КОНТРОЛ КЪМ ДОВЕРИЕ И СТОЙНОСТ: НОВИЯТ МОДЕЛ НА ВЪТРЕШНИЯ ОДИТ

Йоана Чолакова

28 МОЖЕ ЛИ ЕДИН МАЛЪК ОДИТЕН ЕКИП ДА ПОКРИЕ ГОЛЯМА ОДИТНА ВСЕЛЕНА?

Валентина Пенчева

39 СТАНЕТЕ ЧАСТ ОТ СПИСАНИЕ „ВЪТРЕШЕН ОДИТОР“

Изисквания на Редакционния съвет за представяне
на материали за публикуване

ГЛАВЕН РЕДАКТОР -

Д-р инж. Валентина Пенчева, СВОПС

РЕДАКЦИОНЕН СЪВЕТ -

Д-р Светлана Иванова, СВОПС

Димитър Елков, CIA, CRISC, СВОПС

Доц. д-р Светла Бонева-Боянова, CGAP, СВОПС

ГРАФИЧЕН ДИЗАЙН И ПЕЧАТ

Емил Кожухаров

C&M advertising - www.ciem.info

Редакцията на списанието не се ангажира с правото на лично мнение, изразено от авторите в техните статии и публикации.

Разпространяване и препечатване на материали от броя на списание „Вътрешен одитор“ или на части от тях без изричното писмено разрешение на редакцията води до правните последици, предвидени в Закона за авторското право и сродните му права.

Приемат се оригинални ръкописи -
1800 знака на стандартна страница

АДРЕС НА РЕДАКЦИЯТА -

София, ул. Граф Игнатиев 7А, ет.3

тел.: 986 28 08; 981 67 80, факс: 986 28 08

e-mail: iiabulgaria@mbox.contact.bg

СТРАНИЦАТА НА ГЛАВНИЯ РЕДАКТОР

УВАЖАЕМИ ЧИТАТЕЛИ,

В брой 2 за 2026 г. на списание „Вътрешен одитор“ ви представяме материали, посветени на развитието на професията, новите професионални изисквания и практическите предизвикателства пред вътрешния одит.

Броят започва с публикацията **„THE ONE IIA – ЗАЕДНО ГРАДИМ БЪДЕЩЕТО НА ВЪТРЕШНИЯ ОДИТ“**, в която **Цветан Цветков** – председател на Управителния съвет на ИВОБ, и **Димитър Нешев** – директор на ИВОБ, представят основните акценти от заседанието на Общото събрание на Глобалния институт на вътрешните одитори (The IIA), проведено на 20 и 21 юни 2026 г. в Сингапур. Двамата автори участват във форума като представители на Института на вътрешните одитори в България.

Заседанието преминава под мотото „Where it All Comes Together“ и е посветено на визията ONE IIA – обединяване на професионалната общност около общи стандарти, принципи и стратегически цели. Сред водещите приоритети са усъвършенстването на управлението на националните институти, повишаването на професионалната квалификация и сертификацията, привличането на млади специалисти, развитието на публичните политики и нормативното регламентиране на вътрешния одит.

Авторите подчертават прехода от традиционното периодично предоставяне на увереност към по-проактивна роля на вътрешния одит, насочена към предвиждане на рисковете, подпомагане на управлението и защита на общественения интерес. Основното послание е, че бъдещето на професията зависи от общите усилия на вътрешните одитори и от готовността им активно да участват в нейното развитие както в световен мащаб, така и в България.

Следва материалът **„ВЪТРЕШНИЯТ ОДИТ ПРАВИ КРАЧКА НАПРЕД“**, публикуван през април 2026 г. в списание Internal Auditor на The IIA. Неговият автор **Anthony Pugliese** – президент и главен изпълнителен директор на The IIA – разглежда развитието на вътрешния одит като професия, която все по-ясно надхвърля традиционния фокус върху финансовото и нормативното съответствие.

Според него вътрешните одитори все по-често подпомагат организациите при управлението на нововъзникващи рискове, свързани с киберсигурността, изкуствения интелект, устойчивостта и корпоративното управление. Публикацията поставя акцент и върху новите Глобални стандарти за вътрешен одит, „Визия 2035“, развитието на професионалните компетентности и утвърждаването на ролята на вътрешния одит пред регулатори, законодатели и управителни органи. Основното послание е, че професията има перспективно бъдеще, но то изисква своевременна адаптация към променящата се рискова среда.

На практическите аспекти на киберсигурността е посветен материалът **„ИЗИСКВАНИЯТА НА THE IIA ЗА ОДИТ НА КИБЕРСИГУРНОСТТА – ПРАКТИЧЕСКИ НАСОКИ ЗА ВЪТРЕШНИТЕ ОДИТОРИ“**. В него са представени задължителните Cybersecurity Topical Requirements, въведени от The IIA през 2026 г. Те определят минималните изисквания при одити, свързани с киберси-

гурността, както и в случаите, когато в рамките на друг одит бъдат установени значими киберрискове.

Изискванията обхващат управлението на киберсигурността, управлението на киберриска и контролните механизми за защита на информационните активи. Особено значение се отдава на професионалната преценка на вътрешния одитор, документирането на доказателства и обосноваването на евентуални изключения. Целта е да се насърчи по-последователен и надежден подход при оценката на киберрисковете в организациите.

Новите Глобални стандарти за вътрешен одит са във фокуса и на разработката **„ОТ КОНТРОЛ КЪМ ДОВЕРИЕ И СТОЙНОСТ: НОВИЯТ МОДЕЛ НА ВЪТРЕШНИЯ ОДИТ“** с автор **Йоана Чолакова**. Те са представени като съвременна рамка за организацията и изпълнението на одитната дейност, която утвърждава вътрешния одит не само като функция за проверка на съответствието, а като независима и риск-базирана дейност, подпомагаща организацията да постига целите си и да създава стойност.

Стандартите поставят по-силен акцент върху връзката между вътрешния одит, управлението на риска и вътрешния контрол, както и върху отговорността на органите на управление да осигуряват независимост, ресурси и достъп до информация. Наред с това се откроява значението на качеството, етиката, технологичните рискове и използването на данни при изпълнение на одитната дейност.

Практическият опит при стратегическото планиране в лечебно заведение е представен в разработката **„МОЖЕ ЛИ ЕДИН МАЛЪК ОДИТЕН ЕКИП ДА ПОКРИЕ ГОЛЯМА ОДИТНА ВСЕЛЕНА? ПРАКТИЧЕСКИ ПОДХОД ПРИ СТРАТЕГИЧЕСКОТО ПЛАНИРАНЕ НА ВЪТРЕШНИЯ ОДИТ В ЛЕЧЕБНО ЗАВЕДЕНИЕ“** с автор **д-р инж. Валентина Пенчева**. В нея се разглеждат възможностите малък одитен екип да осигури разумно и професионално обосновано покритие на голяма и сложна одитна вселена.

Представен е практически подход за изграждане на одитна вселена, оценка на риска и разработване на тригодишен стратегически план. Акцентът е върху използването на хибриден модел, който съчетава организационните структури и процесите в лечебното заведение, както и върху тематичните и хоризонталните ангажименти като средство за обхващане на взаимосвързани рискове.

Разгледан е и важният въпрос за ресурсните ограничения. Ограничените човекодни са представени като самостоятелен одитен риск, който следва ясно да бъде комуникиран на ръководството. Малкият екип може да предоставя надеждна увереност по най-съществените области, но не може формално да компенсира липсата на ресурс чрез прекомерно разширяване на обхвата или извършване на повърхностни проверки.

Пожелавам ви полезно и приятно четене.

Д-р инж. Валентина Пенчева, СВОПС

THE ONE IIA – ЗАЕДНО ГРАДИМ БЪДЕЩЕТО НА ВЪТРЕШНИЯ ОДИТ

Цветан Цветков – Председател на УС на ИВОБ

Димитър Нешев – Директор на ИВОБ



Цветан Цветков и Димитър Нешев – нашите представители на срещата

В Глобалния институт на вътрешните одитори (The IIA) членуват хора от различни континенти, региони, националности, юрисдикции, сектори и индустрии. Те имат различни традиции и култури, но това, което обединява

всички тях в една общност, е тяхната професия – вътрешен одитор. Професия, която, за да служи наистина на обществения интерес, следва да се упражнява от квалифицирани и непредубедени професионалисти в

съответствие с Глобалните стандарти за вътрешен одит.

Затова и мотото на проведеното на 20 и 21 юни 2026 г. в Сингапур заседание на Общото събрание на The IIA беше „Where it All Comes Together“. Мото, което е в съзвучие и с визията ONE IIA на Глобалния институт, прокламираща постигането на единство на вътрешния одит в различните сектори и правни рамки.

Според The IIA основните компоненти на вътрешния одит следва да бъдат еднакви в целия свят. Те са следните:

- ▶ независимост от оперативното ръководство;
- ▶ прилагане на Глобалните стандарти за вътрешен одит;
- ▶ вътрешните одитори да бъдат квалифицирани и да притежават международно признат сертификат;
- ▶ поне веднъж на пет години да се извършва външна оценка на качеството.

Така се гарантират ефективността на дейността по вътрешен одит и съответствието ѝ с очакванията на заинтересованите страни, независимо дали тя се осъществява в София, Торонто, Кайро или Токио.

Реализацията на тази визия изисква последователни и неуморни усилия от всички филиали на The IIA, отдаденост и прилагане на ясна стратегия както на глобално, така и на национално ниво. Пример за стремежа на общността да функционира като един общ организъм беше над 90-процентното съвпадение на целите в стратегическите планове на националните институти с тези в стратегическия план на Глобалния институт, т.е. постигнато е съгласие за посоката на развитие на вътрешния одит през следващото десетилетие.

Отчетените резултати при изпъл-

нението на тези планове също са повод за гордост и удовлетворение.

Първо, парадигмата на вътрешния одит претърпява съществена трансформация – започна преходът на вътрешния одит от дейност, периодично представяща увереност за процесите по управление, управление на риска и вътрешен контрол в

дясн сертификат.

Трето, значително нараства броят на студентите – членове на института: 10 400, като през 2021 г. те са били 1200, и то само от Северна Америка. Това е резултат и от активното сътрудничество с академичните среди – The IIA е сключил споразумения за сътрудничество със 179 университета.



г-н Цветан Цветков – Председател на УС на ИВОБ

организацията (cyclical assurance), към дейност, подпомагаща проактивно управлението със съвети и мнения (anticipatory governance).

Второ, налице е ясно изразена тенденция на увеличаване броя на националните институти – те вече са 122, като 12 от тях са се присъединили след 2021 г. Продължава да нараства и броят на членовете на The IIA – те вече са 265 000, както и броят на сертифицираните вътрешни одитори – повече от 220 000. Прави впечатление, че сертифицираните одитори са 84% от общия брой на членовете, което илюстрира стремежа на вътрешните одитори по целия свят да демонстрират своята компетентност чрез притежаването на подхо-

Всички тези усилия са подчинени на изпълнението на мисията на Глобалния институт – до 2035 г. вътрешният одит да бъде общо-признат като дейност от първостепенно значение за ефективно управление, управлението на риска и контрола в организацията, а The IIA да бъде водещата глобална институция, предоставяща на вътрешните одитори в целия свят, и най-вече на своите членове, възможността да бъде призната ключовата им роля за отстояване на ценностите на организацията и за нейното развитие и просперитет. През 2026 г. The IIA и националните институти се фокусират върху следните шест приоритета:

1 Предефиниране и трансформация на организационната структура и модела на управление на Глобалния институт и националните институти.

постигането на стратегически-те цели в рамките на 5–6 години. Освен това се препоръчва дефиниране на конфликта на интереси в Етичния кодекс и въвеждане на процедура за докладване и установяване на нарушения на Етичния кодекс.



Отляво надясно: **Javier Faleato** - Executive Vice President Global Institute Relations and Professional Pathways, **Stefano Comotti** -2025-26 IIA Global Board of Directors Chair, **Anthony J. Pugliese** - IIA President and Chief Executive Officer, **Stacey Schabel** - 2026-27 IIA Global Board of Directors Chair, **Benito Ybarra** - Executive Vice President, Global Standards, Guidance and Certifications

Новият модел трябва да се основава на споделени и реципрочни отговорности и задължения между Глобалния институт и националните институти. Традиционният йерархичен модел (top-down) на взаимоотношения се заменя с федеративен – peer-to-peer.

Поставя се задължителното изискване управителният съвет (УС) да бъде от минимум 5 членове, които да са представители на различните сектори. От това следва, че в устава трябва да се регламентира ясна и открита процедура за номиниране и избор на членове на УС. Необходима е ротация на председателя на УС – може би веднъж годишно. Целта на тези промени е да се формира УС, който да е кръг от съмишленици, посветили се на

Предстои всеки национален институт да подпише с Глобалния институт The One IIA Agreement, с което се очертава общата мисия на The IIA и местните институти да работят заедно, за да осигурят динамично лидерство в развитието на интересите на професията на вътрешния одитор посредством стандарти, обучение, сертифициране, провеждане на изследвания и популяризиране на професията по целия свят. Това цялостно споразумение заменя сключваните досега споразумения, засягащи отделни аспекти от дейността на институти-те, като сертификационни програми, обучение, популяризиране на изданията и списанието на Глобалния институт и др.

2 Повишаване на професионалната компетентност и квалификация на вътрешните одитори.

Разработва се нов сертификат в областта на управлението, управлението на риска и контрола с работ-



Отляво надясно: **Javier Faleato** - Executive Vice President Global Institute Relations and Professional Pathways, **Stefano Comotti** -2025-26 IIA Global Board of Directors Chair, **Anthony J. Pugliese** - IIA President and Chief Executive Officer, **Stacey Schabel** - 2026-27 IIA Global Board of Directors Chair, **Benito Ybarra** - Executive Vice President, Global Standards, Guidance and Certifications



Вечеря на участниците в Океанариума. На заден план водолази са разпънали знамето на Глобалния институт.

но заглавие GRC (Governance, Risk, Control). Полагат се усилия Internal Audit Practitioner да се преведе на различни езици в зависимост от броя на желаещите да се явят на изпитите.

Добре познатият сертификат на вътрешните одитори в публичния сектор CGAP отново излиза на сцената, но ще бъде с изцяло ново съдържание.

Новият сертификат IIA Global Quality Certification Program се присъжда на функции по вътрешен одит, които демонстрират изключително съответствие и ефективност съгласно Глобалните стандарти за вътрешен одит.

През 2027 г. ще бъде представен и сертификатът CIA (Challenge Exam Pilot). С него се създава алтернативен път за сертифициране на професионалисти с опит, близък до

одита, като инженери, юристи и др. Кандидатите за сертификати ще преминават 6-седмичен интензивен курс по Глобалните стандарти

за вътрешен одит, етика, оценка на риска и практики за предоставяне на увереност.



Вечеря на участниците в Океанариума



3 Увеличаване на членовете на института и представяне на възможностите за професионално развитие.

Това е константен приоритет на Глобалния институт още от зората на неговото създаване, но сега фокусът е насочен към младите хора, студентите, които са бъдещето на нашата професия. Разширява се и географията на вътрешния одит – в Кения вътрешните одитори са 6 000, което е повече от Италия и почти колкото Франция.

4 Популяризиране на публичните политики и практиките за корпоративно управление на Глобалния институт.

Подготвя се актуализация на Модела на трите линии, която се очаква да бъде публикувана през

2027 г. Подготвя се и проект на позиция за ролята на вътрешния одит в публичния сектор, озаглавен PUBLIC SECTOR GLOBAL PUBLIC POLICY POSITION PAPER. Изготвен е проект и на The role of Internal Audit function in ERM, който понастоящем се обсъжда в професионалната общност.

През 2027 г. ще бъдат издадени следните тематични изисквания, които ще подпомогнат прилагането на Глобалните стандарти: Cybersecurity Topical Requirement, Third-Party Topical Requirement, Organizational Behavior Topical Requirement, Organizational Resilience Topical Requirement, Anti-Corruption, Talent Management, както и следните глобални указания: Understanding Data Analytics for Internal Auditors, Data Analytics Skills for Internal Auditors, Auditing Privacy and Data Protection Risks,

Engagement Planning: Establishing Objectives and Scope.

Други потенциални теми, които ще бъдат обект на публични политики на The IIA, са одитните комитети, рисковете, свързани с измами, рисковете, свързани с изкуствения интелект, ESG и др.

5 Очертаване на перспективите и бъдещите насоки за развитие на професията и нейната роля за защита на обществения интерес.

Вътрешният одит трябва да се развива като дейност, играеща решаваща роля за подобряване на способността на организацията да защитава обществения интерес, и като професия, призвана да служи на обществения интерес. Общественият интерес в своята съвкупност обхваща социалните и иконо-

мическите интереси и цялостното благосъстояние на обществото и организациите.

Глобалният институт подготвя лицензионна програма за предоставяне на своите продукти на външни доставчици на одитни и консултантски услуги. По този начин ще се защити интелектуалната собственост върху продуктите на The IIA, включително GIAS, и ще се осигурят ресурси за изпълнение на мисията.

От 1 януари 2027 г. влиза в сила дисциплинарна и надзорна рамка (THE IIA DISCIPLINARY & OVERSIGHT FRAMEWORK), която изпълнява ценна функция от обществен интерес, като спомага да се гарантира, че некомпетентното, неетичното, неподходящото, непрофесионалното или незаконното поведение от страна на вътрешни одитори и сертифицирани по програмите на The IIA няма да остане без нужно внимание и няма да доведе до накарняване нито на действителната, нито на възприеманата репутация и авторитет на вътрешния одит. Националните институти ще бъдат задължени да я прилагат, защото саморегулацията е привилегия, която трябва да се отстоява.

6 Регламентиране на вътрешния одит в националните законодателства със специален закон или нормативен акт.

За да изпълни своята обществена роля, Глобалният институт препоръчва вътрешният одит в отделните страни и региони да бъде законово регламентиран, а националните институти да бъдат гаранتي, че той ще се развива като саморегулираща се професия без политически натиск или влияние.

Това е формулирано като цели в позицията на Института „THE GLOBAL PUBLIC POLICY POSITION

PAPER GP 4“, която е фундаменталната база, въз основа на която трябва да се провеждат инициативите и форумите за популяризиране на вътрешния одит.

Пет са основополагащите изисквания в този документ:

1. Устройството и организацията на вътрешния одит да бъдат регламентирани със специален закон или нормативен акт.
2. Приемане и прилагане на Глобалните стандарти за вътрешен одит като единствените стандарти за ефективен вътрешен одит.
3. Въвеждане на вътрешния одит във всички сектори от обществен интерес, включително и в компаниите, търгуващи с криптовалута.
4. Професията „вътрешен одитор“ да се развива като саморегулираща се професия, призната с нормативен акт или от компетентен регулаторен орган.
5. Организацията и дейността на националния институт на вътрешните одитори в някои аспекти, като взаимодействието с одитните комитети, да бъдат съобразени с тези на професионалните организации на регистрираните одитори и счетоводителите.

Очертаните стратегически приоритети показват, че вътрешният одит днес е на нов етап от еволюционното си развитие. Дали ще успее да отговори на очакванията на обществото да бъде ключов фактор за добро управление и създаване на стойност, зависи от вътрешните одитори от различните страни, региони и сектори. Зависи от готовността им да напуснат комфортната зона и заедно да градят своето бъдеще. Нека не чакаме покана, нека заедно да започнем да градим бъдещето на вътрешния одит в България.



ВЪТРЕШНИЯТ ОДИТ ПРАВИ КРАЧКА НАПРЕД

След пет години на развитие президентът и главен изпълнителен директор на The IIA **Anthony Pugliese** е фокусиран върху бъдещето на професията.

Професията на вътрешния одитор винаги е била глобална, разнообразна и тясно свързана с организациите, които подпомага. Когато преди пет години поех ръководството на The Institute of Internal Auditors (The IIA), един от първите ми приоритети беше разработването и прилагането на по-глобална стратегия за управление,

която по-добре да отразява международния обхват на нашата професия.

Днес The IIA е световна федерация, обединяваща повече от 170 държави – и продължава да се разраства – като всяка от тях е представена от национален институт. През последните години насочихме усилията си към по-тясно сътрудничество с националните институти и изграждането

на стратегически план, който да отговаря на потребностите на членовете ни по целия свят. Благодарение на тези усилия The IIA се утвърди като истински глобална организация, способна да отразява многообразието на професията и да откликва на непрекъснато променящите се потребности на вътрешните одитори по света.

В този период на промени

едно остана непроменено – вътрешните одитори продължават да бъдат професионалистите, които имат най-пълна представа за случващото се в цялата организация. Заради тази уникална перспектива ролята на вътрешния одит се разширява по естествен път – от оценката на нововъзникващи рискове до предоставянето на стратегически консултации.

Професията се развива, очакванията към нея нарастват, а възможностите пред нея са значителни. Тези тенденции потвърждават една проста истина – вътрешният одит не просто запазва своето значение, а продължава успешно да се развива.

ВАЖНА ПРОМЯНА

За да продължи напред с единен подход към професионалната практика, през 2024 г. The IIA въведе новите Глобални стандарти за вътрешен одит – най-цялостната актуализация правена някога на Международните стандарти за професионалната практика по вътрешен одит. Убедени бяхме, че предизвикателствата, пред които вътрешните одитори бяха изправени това десетилетие и вероятно



ще срещат в бъдеще, изискват нов поглед към професионалните стандарти. Международният съвет по стандартите за вътрешен одит разработи новите изисквания, отчитайки динамичната бизнес среда и все по-сложния рисков профил на организациите.

Новите стандарти предоставят ясна рамка за предоставяне на висококачествени услуги за даване на увереност и за консултиране. Те формулират основните принципи, задължителните изисквания и насоките за тяхното прилагане в по-ясен и практически ориентиран формат. Още по-важно е, че затвърждават ролята на вътрешния одит като ключов партньор на одитните комитети, съветите на директорите, висшето ръководство и останалите заинтересовани страни.

Участието в разработването на тези стандарти беше изключително удовлетворяващ процес. Осъзнавахме, че чрез тяхното модернизиране предоставяме на членовете на професията по-ясни насоки как да „изпреварват“ нововъзникващите рискове, преди те да доведат до неблагоприятни последици. Макар да са в сила едва от година, първоначалните резултати показват, че вече оказват реална практическа полза. По-широката ни цел е да модернизираме професията, като я подготвим за съвременните рискове и да

утвърдим вътрешния одит като стратегически партньор на организациите.

НОВА ВИЗИЯ

В средата на 2024 г. Фондацията за вътрешен одит публикува доклада **„Вътрешен одит: Визия 2035“**, който представя цялостна визия за развитието на професията.

Изготвен въз основа на мненията на хиляди професионалисти и заинтересовани страни от 155 държави, докладът очертава пътна карта за бъдещото развитие на вътрешния одит.

Изследването прави един основен извод, който е напълно категоричен: вътрешният одит трябва да се трансформира още сега, в противен случай съществува риск да загуби своята значимост до 2035 г.

За да се осъществи тази трансформация, професията трябва да:

- промени обществените възприятия за вътрешния одит;
- възприеме новите технологии;
- разшири обхвата на своята дейност;
- свърже по-тясно вътрешния одит със стратегическите цели на организациите;
- развива и привлича нови професионални кадри.

Визия 2035 вече служи като стратегическа пътна карта за развитието на

професията, очертавайки пътя как вътрешните одитори да останат актуални през следващото десетилетие и след това. Това означава по-активно участие в консултантски дейности, съобразени със стратегическите приоритети, както са определени от ръководството, съвета и одитните комитети. The IIA е ангажиран с реализирането на целите, очертани във Визия 2035 чрез процеса на нашето стратегическо планиране за по-нататъшното развитие и укрепване на професията в световен мащаб.

В подкрепа на тази визия The IIA създаде Комитет за управление на корпоративния риск (Enterprise Risk Management Committee), чиято задача е да потвърди изводите от изследването „Визия 2035“, да анализира променящата се среда на управление на риска и да оцени стратегическите възможности за развитие в рамките на екосистемата на функциите за даване на увереност. Досега обсъжданията на Комитета са допринесли за актуализацията на Модела на трите линии и са оформили дискусии относно ролята на The IIA в подкрепа на професионалистите в областта на корпоративното управление, управлението на риска и съответствието в световен мащаб.

ОТВЪД ЦИФРИТЕ

Като се отдръпна назад, за да погледна по-широката картина, виждам

ясната еволюция, която вътрешният одит претърпява. В някои организации вътрешният одит е функция за финансово и нормативно съответствие. Все по-често обаче заинтересованите страни очакват той да обхваща и нововъзникващите рискове.

Днес много функции за вътрешен одит работят в области, които далеч надхвърлят цифрите, играейки ключова роля в области като киберсигурност, организационно поведение и организационна устойчивост.

Изкуственият интелект също променя професията. Той е едновременно мощен инструмент, който подобрява начина, по който вътрешните одитори извършват своята работа, и като област, в която вътрешният одит има съществена роля при подпомагането на заинтересованите страни да разбират, управляват и използват тази технология по отговорен начин.

Що се отнася до киберсигурността, е очевидно, че заплахите стават все по-сложни, което означава, че и вътрешните одитори трябва непрекъснато да развиват своите компетентности. В отговор на това The IIA публикува Тематично изискване в областта на киберсигурността (Cybersecurity Topical Requirement), което очертава основните въпроси, свързани с управлението, риска и

контрола, които следва да бъдат разглеждани при извършване на одитен ангажимент в тази област.

Тематичните изисквания дават увереност на регулаторите и останалите заинтересовани страни за това как широко разпространените и устойчиви рискове се идентифицират, контролират и управляват по последователен начин.

Нашата професия има дългогодишен опит в успешното адаптиране към променящите се изисквания на заинтересованите страни и на регулаторите, както и към развитието на технологиите, пазара на труда и бизнес процесите. За да отговори на тези изисквания, The IIA прилага структуриран, но достатъчно гъвкав стратегически подход, който определя както настоящите ни действия, така и бъдещата посока на развитие.

През следващото десетилетие вътрешният одит ще претърпи по-нататъшна трансформация, водена от ускоряващия се технологичен напредък, революционните тенденции и нововъзникващите рискове. Както е посочено във Визия 2035, тази еволюция ще изисква нови умения, по-силен набор от таланти и повишено доверие, за да се одитират ефективно нови и нововъзникващи рискове и да се обслужва общественият интерес.

ГЛОБАЛЕН РАСТЕЖ

The IIA стигна до това заключение отдавна: Ако не се развиваме, не се разширяваме и не растем, ще изостанем. Поради това промените през последните пет години доведоха до присъединяването на 35 000 нови членове, с което общият ни брой вече надхвърля 265 000.

Същевременно международното присъствие на The IIA продължава да се разширява. Само за пет години бяха създадени 14 нови национални института, а през последната година такива бяха учредени в Грузия, Мексико, Намибия, Пакистан и Узбекистан.

Освен това, нашите национални институти в Близкия изток си партнираха с The IIA, за да създадат Арабската конфедерация на институтите на вътрешните одитори (ARABICIIA) в подкрепа на бързо разрастващата се професия в региона. Краткосрочната цел на Института е да достигне 300 000 членове по целия свят.

Нашата цел в растежа е да отговорим по-добре на нуждите на вътрешните одитори по целия свят – включително много от тези, които все още не са членове – като същевременно засилим колективния си глас в защита на професията. Този растеж изисква The IIA да бъде по-внимателен

относно това, което прави, като същевременно остане фокусиран върху променящия се характер на нашата професия. Не можем да чакаме да действаме и след това да реагираме; вместо това трябва да предвиждаме промените.

Този подход накара Института да преработи нашия модел на членство. Преди това имашме универсален подход, който изглеждаше остарял и безличен. Днес нашият модел е по-съобразен, особено за по-младите професионалисти, които искат да знаят как членството в The IIA може да им бъде от полза. Искаме да направим повече от това просто да говорим за чувството си за общност; искаме да демонстрираме силата на това да бъдеш част от глобална мрежа от професионалисти.

Надеждата ми за бъдещето на The IIA е да продължи траекторията на растеж дълго след моя мандат като президент и главен изпълнителен директор. Подготвяме професията за бъдещето с инициативи, които гарантират, че ще има квалифицирани хора, навлизащи в професията по целия свят, от студенти до хора, които са в средата на кариерата си.

За да подготви тези специалисти, The IIA актуализира изпита за сертифициран вътрешен одитор (CIA), за да отрази новите стандарти и да се съсредоточи върху

прилагането на основните одиторски компетенции. Също така направихме квалификацията „Сертифициран вътрешен одитор“ (IAP) постоянна част от програмата за сертифициране и първата стъпка за полагане на изпита CIA. IAP дава на студентите и новите вътрешни одитори начин да демонстрират своите способности и път към постигане на нашия водещ сертификат CIA.

Надграждайки тези пътища за акредитация, The IIA разработва цялостна образователна екосистема за обучение, като разширява партньорствата и стартира програми, като например AI-Enabled Coordinated Assurance Certificate, предназначена да подпомага ръководителите на звената за вътрешен одит в придобиването на ключови компетентности за работа в условията на използване на изкуствен интелект. В подкрепа на тази стратегия, Екипът за компетентност и обучение на членовете внедри единна технологична платформа, която обединява конференциите, обученията и вебинарите, като улеснява регистрацията, плащанията, отчетността и цялостното участие на членовете.

В същото време, подобренията и автоматизацията на процесите – включително преработен работен процес за продължаващо професионално обучение, който намали

издаването на кредити от около 60 дни на три дни или по-малко – подобри ефективността и удовлетвореността на членовете. Всички тези инициативи модернизират начина, по който IIA предоставя своите услуги, улесняват участниците в професионалните събития и укрепват последователността и надеждността на глобалната мрежа на Института.

ЗАСТЪПВАНЕ ЗА ПРОФЕСИЯТА

За мен застъпничество то означава The IIA да присъства навсякъде, където се обсъжда вътрешният одит – а също и там, където би трябвало да се обсъжда, но все още не е. Гласът на професията трябва да се чува не само в рамките на организациите, но и сред законодателите, регулаторните органи и лидерите на общественото мнение.

Създаването на специализиран екип по застъпничество е сравнително ново направление в дейността на The IIA, но вече дава осезаеми резултати в различни части на света. През последните пет години нашите усилия бяха насочени към утвърждаване на ролята на вътрешния одит в дискусиите, свързани с изкуствения интелект, криптоактивите, защитата на личните данни и корпоративното управление.

Global Public Policy Position Paper (GP4) на

The IIA – това е документ, който формулира единна позиция на Института за застъпничеството за професията на вътрешен одит по света. Приет през 2024 г., той определя основните приоритети и подпомага националните институти да представят последователни и аргументирани позиции пред законодателните и регулаторните органи в своите държави.

За да подкрепи тези институти, The IIA е избрал да присъства на местата, където това има най-голямо значение. Например в Африка беше стартирана специална инициатива за популяризиране на значението и въздействието на вътрешния одит на континента, включително чрез разработването на примерни законодателни решения.

В Канада The IIA подкрепи изменение на Закона за защита на критичните киберсистеми, което впоследствие беше одобрено от Постоянната комисия по обществена безопасност и национална сигурност към Камарата на общините. Изменението ясно определя ролята на вътрешния одит и признава Международната рамка за професионални практики, като по този начин подчертава значението на независимото осигуряване, основано на международните стандарти, за защитата на критичната инфраструктура.

Убедени сме, че чрез активното си застъпване

През следващото десетилетие вътрешният одит ще претърпи по-нататъшна трансформация, движена от ускоряващия се технологичен напредък, променящите правилата на играта тенденции и възникващите рискове.

за професията The IIA може да допринесе за по-доброто разбиране на жизненоважната роля на вътрешния одит. Именно с тази цел беше създаден Global Audit Committee Center – инициатива, насочена към повишаване на авторитета и влиянието на вътрешния одит в работата на одитните комитети и управителните органи.

Центърът ще предоставя на членовете на одитните комитети актуална информация за приноса и добрите практики на професията.

The IIA активно участва и в обсъждането на проектозаконодателството на Съединените щати относно криптоактивите, като предложи включването на изрични препратки



към ролята на вътрешния одит в Digital Asset Market Clarity Act, приет от Камарата на представителите през юли 2025 г.

През 2023 г. Институтът успя да убеди Съвета за надзор върху счетоводството на публичните дружества в САЩ (PSAOB) да премахне текст от Одиторски стандарт 2310, който ограничаваше участието на вътрешния одит в процеса на потвърждаване на информацията. В актуализираната редак-

засилват независимостта на вътрешния одит и утвърждават неговата роля както в работата на управителните органи, така и при формирането на публичните политики.

The IIA е наясно, че общественото разбиране за професията все още представлява едно от най-сериозните предизвикателства. Много хора продължават да не познават реалната работа на вътрешните одитори или имат неточна представа

БЪДЕЩЕТО Е НАШЕ

Всеки ден, когато вземаме решения от името на стотиците хиляди членове на The IIA, си давам сметка за огромната отговорност, която носим като пазители и двигатели на една професия, чието значение непрекъснато нараства. Това чувство на отговорност никога не се превръща в рутина. То постоянно ми напомня колко важна е работата, която вършим в The IIA.

развиваме професията, да укрепваме стандартите, да подкрепяме нашите членове и да гарантираме, че вътрешният одит ще бъде подготвен да посреще предизвикателствата на времето. Именно тази отговорност поражда силна мотивация, която се споделя от нашите служители, доброволци, национални институти и цялата ни международна общност. Тя е движеща сила за напредъка.

След пет години начело на The IIA съм по-убеден

В своята съвкупност тези усилия за застъпничество насърчават доброто управление, утвърждават независимостта и засилват ролята на вътрешния одит в управителните съвети и в сферата на публичните политики в световен мащаб.

ция на PSAOB вече изрично се признава ключовата роля на вътрешния одит в одиторския процес.

Освен това The IIA въведе Рамка за дисциплинарни мерки и надзор, която гарантира справедлив и прозрачен процес за разглеждане на сигнали и нарушения, свързани с професионалното поведение на вътрешните одитори.

В своята съвкупност тези инициативи укрепват системите за корпоративно управление,

за това, което правим.

Подобно на самата професия, и The IIA се стреми да бъде възприеман като модерна, актуална и ориентирана към бъдещето организация – от своя интернет сайт до конференциите и всички точки на взаимодействие с членовете си. Поради това Институтът продължава да модернизира своите основни системи и процеси, така че те да отговарят по-пълно на потребностите на професионалната общност.

От първо лице виждам колко големи възможности се откриват пред нашата професия и чувам същото при срещите си с наши членове по целия свят. Организацията работят в среда на все по-голяма сложност, по-бързи промени и непрекъснато растящи очаквания, а вътрешните одитори са уникално позиционирани, за да им помогнат да се справят с тези предизвикателства.

Тези възможности носят и сериозна отговорност – да продължим да

от всякога, че бъдещето на вътрешния одит е стабилно и перспективно и че заедно ще продължим да развиваме професията. Никога досега не е имало по-подходящ момент човек да бъде вътрешен одитор.

Anthony Pugliese, CIA, CPA, CGMA, CITP, е Президент и Главен изпълнителен директор на The IIA.

Превода направи за Вас: д-р Светлана Иванова, СВОПС

Член на ИВОБ



NEW! The IIA's Financial
Services Audit Certificate

Learn More



ИЗИСКВАНИЯТА НА THE IIA ЗА ОДИТ НА КИБЕРСИГУРНОСТТА – ПРАКТИЧЕСКИ НАСОКИ ЗА ВЪТРЕШНИТЕ ОДИТОРИ



1. Въведение

През 2025 г. Институтът на вътрешните одитори (IIA) публикува документа Cybersecurity Topical Requirement (Тематично изискване в областта на киберсигурността) като част от обновената Международна рамка за професионална практика (IPPF). Новата рамка включва Глобалните стандарти за вътрешен одит, тематичните изисквания и глобалните насоки. Изискванията влязоха в сила от 5 февруари 2026 г.

Документът въвежда задължителни минимални изисквания при извършване на ангажименти за даване на увереност, свързани с киберсигурността. Основната цел е да се постигне по-голяма последователност, качество и надеждност в работата на вътрешните одитори при оценката на киберрисковете.

Следва ясно да се разграничават двата документа, публикувани от IIA:

- ▶ Cybersecurity Topical Requirement съдържа задължителните минимални изисквания;
- ▶ Ръководството за прилагане, има подпомагаш характер и предоставя практически насоки, примери и разяснения относно прилагането на изискванията.

IIA изрично подчертава, че Topical Requirement не представлява цялостна програма за одит на киберсигурността, а минимална базова рамка. В зависимост от рисковия профил на организацията може да бъде необходимо включването на допълнителни проверки, контроли и одитни процедури.

2. Кога изискванията са задължителни

IIA определя три случая, при които Topical Requirement следва задължително да бъде приложен:

- ▶ когато киберсигурността е предмет на ангажимент, включен в годишния одитен план;
- ▶ когато по време на друг ангажимент бъдат установени киберрискове;
- ▶ когато бъде поискан извънпланов ангажимент, свързан с киберсигурността.

Практическото значение на това изискване е съществено. Приложимостта не се ограничава единствено до специализирани ИТ одити. Киберрискове могат да бъдат установени и при проверки на финансови, оперативни или административни процеси.

В Cybersecurity Topical Requirement User Guide (Ръководство за прилагане на Тематичното изискване в областта на киберсигурността) е представен пример с одит на процеса по разплащания към доставчици. Първоначално киберсигурността не е включена в обхвата на проверката, но след преглед на процеса вътрешните одитори установяват рискове, свързани с електронното подаване на заявки за покупки. Това налага прилагането на Topical Requirement.

На практика това означава, че вътрешните одитори трябва:

- ▶ да разпознават киберрискове и извън традиционните ИТ процеси;
- ▶ да адаптират обхвата на ангажимента при промяна на рисковия профил;



- ▶ да документират основанията за всяко изключено изискване.

3. Значението на професионалната преценка

И двата документа поставят силен акцент върху професионалната преценка на вътрешния одитор. Решението кои изисквания са приложими зависи от:

- ▶ оценката на риска;
- ▶ обхвата на конкретния ангажимент;
- ▶ зрелостта на организацията;
- ▶ характера и значимостта на киберрисковете.

Не всички изисквания са приложими във всеки ангажимент. Например дадена проверка може да бъде ограничена само до управлението на потребителския достъп или до реакцията при инциденти. Вътрешните одитори следва:

- ▶ да оценят приложимостта на всяко изискване;
- ▶ да документират причините за евентуалното му изключване;
- ▶ да съхраняват доказателства за направената оценка.

Това е особено важно при оценки на качеството на

одитната дейност, тъй като съответствието с Topical Requirements подлежи на проверка.

4. Корпоративно управление на киберсигурността

Първата група изисквания е свързана с процесите по управление на киберсигурността. Основният акцент е поставен върху наличието на формализирана стратегия, ясно разпределени отговорности и активно участие на ръководството.

4.1. Стратегия и цели

Вътрешните одитори следва да оценят:

- ▶ дали организацията има официално утвърдена стратегия за киберсигурност;
- ▶ дали стратегията се актуализира периодично;
- ▶ дали управителният орган получава регулярна информация за напредъка, необходимите ресурси и бюджета.

Ръководството за прилагане посочва като възможни доказателства:

- ▶ показатели за изпълнение;
- ▶ отчети за коригиращи действия;

- ▶ бюджетни анализи;
- ▶ информация за необходимите човешки ресурси.

Практическите проверки могат да включват:

- ▶ протоколи от заседания;
- ▶ отчети на ръководителя по информационна сигурност;
- ▶ стратегически планове;
- ▶ бюджети и инвестиционни програми.

4.2. Политики и процедури

Изисква се наличие на политики и процедури, които:

- ▶ са официално утвърдени;
- ▶ се преглеждат поне веднъж годишно;
- ▶ подпомагат контролната среда.

IIA препоръчва използването на широко разпространени рамки като:

- ▶ NIST;
- ▶ COBIT;
- ▶ други приложими стандарти и методологии.

Практическите проверки могат да включват:

- ▶ проследяване на промените в политиките;
- ▶ оценка дали процедурите се прилагат реално;
- ▶ управление на изключенията и отклоненията.

4.3. Роли и отговорности

Организацията следва ясно да е определила:

- ▶ ролите и отговорностите;
- ▶ подчинеността на функциите по киберсигурност;
- ▶ процес за оценка на знанията и уменията на служителите.

Практическите проверки могат да включват:

- ▶ длъжностни характеристики;
- ▶ планове за обучение;
- ▶ професионални сертификати;
- ▶ организационна структура.

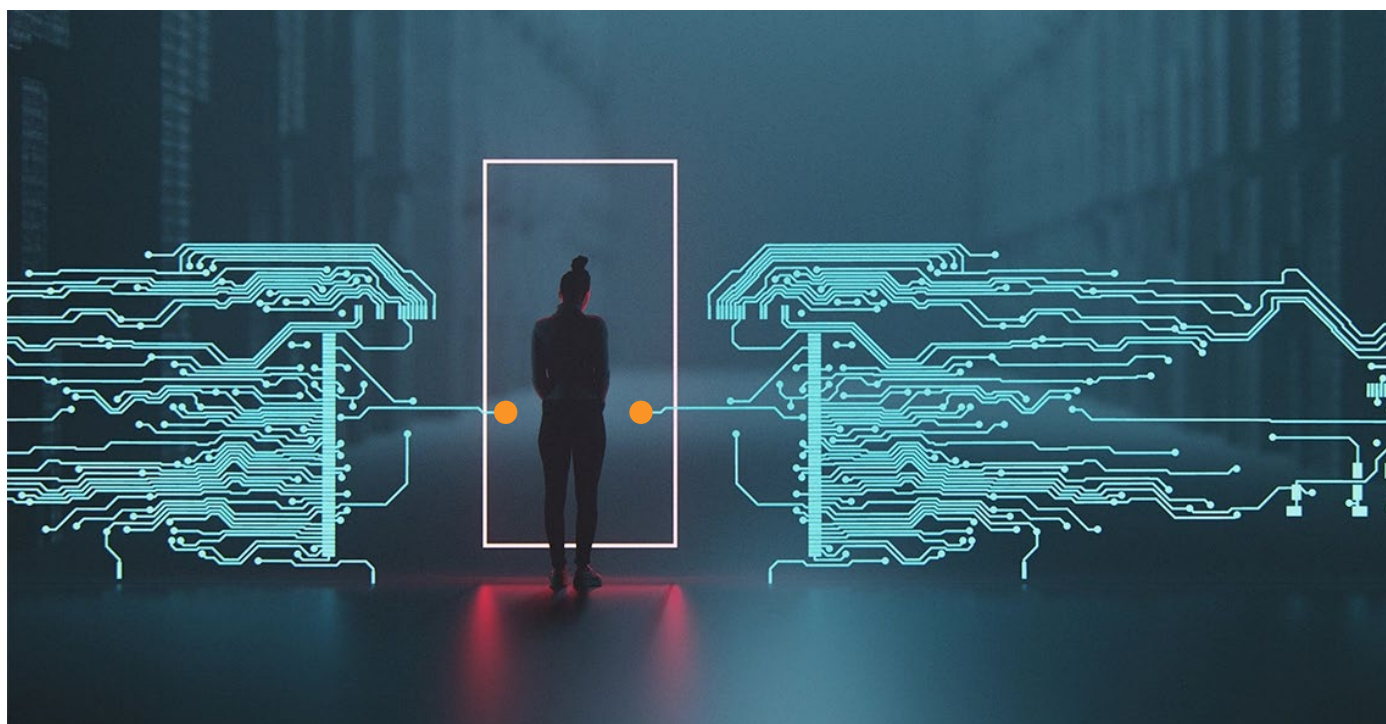
4.4. Участие на заинтересованите страни

Документът подчертава необходимостта от взаимодействие между:

- ▶ ръководството;
- ▶ оперативните звена;
- ▶ управлението на риска;
- ▶ човешките ресурси;
- ▶ правните функции;
- ▶ звената по съответствие;
- ▶ външните доставчици.

Вътрешният одитор може да търси доказателства под формата на:

- ▶ протоколи от срещи;
- ▶ доклади;
- ▶ кореспонденция;
- ▶ решения на комитети.



5. Управление на киберриска

Втората група изисквания е насочена към процесите по идентифициране, оценка, управление и наблюдение на киберрисковете.

5.1. Идентифициране и наблюдение на рисковете

Организацията трябва да разполага с процеси за:

- ▶ идентифициране на заплахи и уязвимости;
- ▶ анализ на риска;
- ▶ предприемане на мерки за ограничаване;
- ▶ текущо наблюдение на рисковете.

Практическите доказателства могат да включват:

- ▶ регистри на рисковете;
- ▶ оценки на уязвимости;
- ▶ планове за коригиращи действия;
- ▶ периодични отчети.

5.2. Участие на различни функции

ИА подчертава, че управлението на киберриска не е единствено отговорност на ИТ звеното. В процеса трябва да участват:

- ▶ управление на риска;
- ▶ правни функции;
- ▶ човешки ресурси;
- ▶ финанси;
- ▶ оперативни звена;
- ▶ управление на веригата на доставки.

Практически вътрешният одитор следва да оцени:

- ▶ дали има координиран подход;
- ▶ дали информацията за риска се обменя между функциите;
- ▶ дали има механизми за съвместно вземане на решения.

5.3. Отговорности и докладване

Документът изисква:

- ▶ определяне на отговорно лице или екип;
- ▶ периодично докладване;
- ▶ наблюдение на нововъзникващи заплахи.

Проверките могат да обхванат:

- ▶ разпределението на отговорностите;
- ▶ процесите за докладване;
- ▶ механизмите за ескалиране;
- ▶ периодичността на отчетите към ръководството.

5.4. Ескалиране на риска

Особено внимание е отделено на:

- ▶ нивата на риск;
- ▶ критериите за ескалиране;
- ▶ финансовите и нефинансовите последици;
- ▶ нормативните изисквания.

Практически вътрешният одитор може да провери:

- ▶ методиката за определяне на критичност;
- ▶ сроковете за уведомяване;
- ▶ комуникационните процедури;
- ▶ връзката с общото управление на риска.

5.5. Осведоменост и обучения

Организацията следва да провежда:

- ▶ периодични обучения;
- ▶ симулирани фишинг атаки;
- ▶ кампании за повишаване на осведомеността.

Като доказателства могат да бъдат използвани:

- ▶ отчети за преминати обучения;
- ▶ резултати от тестове;
- ▶ статистика за потребителското поведение;
- ▶ коригиращи действия.

5.6. Реакция при инциденти и възстановяване

ИА изисква наличие на:

- ▶ план за реакция при инциденти;
- ▶ процедури за ограничаване на въздействието;
- ▶ процедури за възстановяване;
- ▶ анализ след инцидент;
- ▶ периодично тестване.

Практическите проверки могат да включват:

- ▶ документация от тестове;
- ▶ регистри на инциденти;
- ▶ анализи на причините;
- ▶ проследяване на изпълнението на препоръките.

6. Контролни процеси

Третата група изисквания е свързана с конкретните контролни механизми.

6.1. Вътрешни и външни контроли

Организацията трябва да гарантира защита на:

- ▶ поверителността,
- ▶ целостта и
- ▶ наличността на информацията и системите.

Ръководството за прилагане обръща внимание и на:

- ▶ докладите за контроли при доставчици;
- ▶ тестове за проникване;
- ▶ проследяване на слабости и коригиращи действия.

6.2. Управление на човешките ресурси

Изисква се процес за:

- ▶ обучение;
- ▶ развитие на компетентности;
- ▶ професионално развитие;
- ▶ обмен на знания.

6.3. Непрекъснато наблюдение

Организацията следва да наблюдава:

- ▶ нововъзникващи заплахи;
- ▶ уязвимости;
- ▶ рискове, свързани с нови технологии, включително изкуствен интелект.

6.4. Управление на жизнения цикъл на активите

IIA поставя акцент върху управлението на:

- ▶ хардуер;
- ▶ софтуер;
- ▶ услуги на доставчици;
- ▶ извеждане от експлоатация.

Ръководството посочва тези контроли като примери за мерки за защита на активите в различните етапи от жизнения цикъл:

- ▶ криптиране;
- ▶ антивирусна защита;
- ▶ виртуални частни мрежи;
- ▶ актуализация на системи;
- ▶ контроли върху бази данни;
- ▶ интегриране на сигурността в процеса по разработка на софтуер.

6.5. Мрежова и крайна защита

Минималната рамка включва:

- ▶ многофакторна автентикация;
- ▶ управление на потребителски достъп;
- ▶ сегментиране на мрежите;
- ▶ защитни стени;
- ▶ системи за откриване и предотвратяване на атаки;
- ▶ защита на облачни и комуникационни услуги.

Практически това насочва вътрешния одитор към

проверка на:

- ▶ управлението на достъпа;
- ▶ отдалечения достъп;
- ▶ конфигурацията на мрежите;
- ▶ контрола върху обмяна на файлове;
- ▶ механизмите за наблюдение.

7. Документиране и доказване на съответствие

Документите многократно подчертават необходимостта от:

- ▶ подход, основан на доказателства;
- ▶ документиране на приложимостта;
- ▶ аргументиране на изключенията.

На практика документирането на изключения може да включва кратко описание защо дадено изискване не е приложимо в конкретния ангажимент. Например вътрешният одитор може да посочи, че определени мрежови контроли не са включени в обхвата, тъй като проверката е ограничена до управление на потребителски достъп или до оценка на реакцията при инциденти. Подобни решения следва да бъдат аргументирани и съхранявани като част от одитната документация.

Практическата стойност на този подход е значителна, защото:

- ▶ улеснява оценките на качеството;
- ▶ осигурява проследимост;
- ▶ подпомага последователността между ангажиментите;
- ▶ позволява защита на професионалната преценка.

8. Връзка с NIST CSF 2.0, COBIT 2019 и NIST SP 800-53

Ръководството за прилагане съдържа съпоставка между изискванията на документа и:

- ▶ NIST Cybersecurity Framework 2.0;
- ▶ COBIT 2019;
- ▶ NIST SP 800-53.

Това има важно практическо значение, тъй като много организации вече използват тези рамки при изграждането на своята система за информационна сигурност.

Документът препоръчва вътрешните одитори да съгласуват съществуващите си одитни програми с изискванията на Topical Requirement, така че да се гарантира достатъчно покритие на риска.

9. Заключение

Cybersecurity Topical Requirement на IIA въвежда единна минимална рамка за оценка на управлението, управлението на киберриска и контролните процеси в областта на киберсигурността.

Основната практическа стойност на документа се състои в:

- ▶ формализира очакванията към вътрешния одит;
- ▶ въвежда последователен подход при оценката на киберрисковете;
- ▶ поставя изискване за доказуема приложимост и документация;
- ▶ интегрира киберсигурността в основаното на риска вътрешно одитиране.

Документът разглежда киберсигурността не само като технологичен въпрос, а като организационен процес, който изисква участие на ръководството, координация между различни функции и непрекъснато наблюдение на риска.

За вътрешните одитори това означава необходимост от:

- ▶ по-широко разбиране на киберриска;
- ▶ адаптиране на одитните програми;
- ▶ по-задълбочено документиране;
- ▶ активно прилагане на професионална преценка при определяне на обхвата и приложимостта на изискванията.

Редакционен екип на сп. „Вътрешен одитор“



ОТ КОНТРОЛ КЪМ ДОВЕРИЕ И СТОЙНОСТ: НОВИЯТ МОДЕЛ НА ВЪТРЕШНИЯ ОДИТ

Какво е различното в новите Глобални стандарти за вътрешен одит?

Йоана Чолакова, СВОПС – член на ИВОБ

Новите Глобални стандарти за вътрешен одит не представляват просто редакция на предходните професионални изисквания. Те предлагат по-цялостен модел за позициониране, управление и изпълнение на вътрешния одит, съобразен с нарастващата сложност на организационната среда, динамиката на рисковете, технологичното развитие и обществените очаквания за прозрачност и отговорност.

Основната промяна е в разбирането за предназначението на вътрешния одит. Той не се разглежда единствено като контролна или проверяваща функция, а като независима професионална дейност, която подпомага организацията да създава, защитава и поддържа стойност. Това се осъществява чрез обективна оценка на управлението, управлението на риска и вътрешния контрол, както и чрез предоставяне на обосновани препоръки, наблюдения и перспектива за бъдещи предизвикателства.

1. ОТ СЪОТВЕТСТВИЕ КЪМ РЕАЛЕН ПРИНОС ЗА ПОСТИГАНЕ НА ЦЕЛИТЕ

Предишната професионална рамка също поставяше изисквания за качество, независимост, управление на риска и контрол. Новите стандарти обаче по-ясно свързват дейността на вътрешния одит с постигането на стратегическите и оперативните цели на организацията.

Вътрешният одит следва не само да установява дали дадени правила, процедури и контролни механизми съществуват и се прилагат. Той трябва да оценява дали те действително подпомагат организацията да постига своите цели, да използва ресурсите разумно, да управлява рисковете своевременно и да реагира адекватно на настъпващи промени.

Този подход е приложим във всички сектори. В търговска или производствена организация фокусът може да бъде върху ефективността на веригата на доставки, управлението на запасите, договорните отношения и финансовата устойчивост. В енергийно или газоразпределително дружество той може да се отнася до сигурността и непрекъсваемостта на доставките, управлението на техническите активи, инвестиционните проекти и спазването на изискванията за безопасност. В лечебно заведение може да е свързан с надеждността и устойчивостта на процесите по лекарствено снабдяване, отчетност и защита на медицинската информация.

2. ПО-ЯСНА ОТГОВОРНОСТ НА ОРГАНИТЕ НА УПРАВЛЕНИЕ И ВИСШЕТО РЪКОВОДСТВО



Една от най-съществените характеристики на новите стандарти е по-ясното определяне на ролята на органите на управление и висшето ръководство за ефективността на вътрешния одит.

Вътрешният одит не може да бъде ефективен само чрез усилията на одиторите. Необходимо е органът, който упражнява надзор, и висшето ръководство да осигуряват условия за неговата независимост, подходящо организационно позициониране, доста-

тъчни ресурси, достъп до информация и възможност за пряка комуникация по значими рискове и констатации.

Така вътрешният одит се утвърждава като елемент от системата на добро корпоративно и публично управление, а не като изолирана административна функция. Същевременно той запазва своята независимост и не следва да поема управленски отговорности или да взема решения вместо ръководството.

3. ЕДИННА И ПО-ПРАКТИЧНА СТРУКТУРА НА ПРОФЕСИОНАЛНАТА РАМКА



Новите стандарти са организирани в пет взаимосвързани области:

1. предназначение на вътрешния одит;
2. етика и професионализъм;
3. управление на функцията по вътрешен одит;
4. управление на дейността по вътрешен одит;
5. изпълнение на вътрешни одитни ангажименти.

Тази структура създава по-ясна логическа връзка между професионалните ценности, независимостта, стратегическото планиране, осигуряването на ресурси, качеството на одитната дейност и изпълне-

нието на конкретните ангажименти.

Към всяко изискване са предвидени насоки за прилагане и примери за доказателства за съответствие. Това подробно е описано в преводната статия, изготвена от The IIA, „ИНСТРУМЕНТ ЗА ОЦЕНКА НА ГОТОВНОСТТА ЗА СЪОТВЕТСТВИЕ“, публикувана в бр. 2 на списание „Вътрешен одитор“ от 2025 г. Това улеснява практическото прилагане на стандартите и е особено полезно за по-малки одитни звена, които трябва едновременно да поддържат качество, да покриват значима одитна вселена и да работят при ограничен ресурс.

4. ПО-СИЛЕН АКЦЕНТ ВЪРХУ ОБЩЕСТВЕНИЯ ИНТЕРЕС, ЕТИКАТА И ДОВЕРИЕТО



Новите стандарти изрично поставят дейността по вътрешен одит в контекста на обществения интерес. Това има особено значение за публичните организации, лечебните заведения, дружествата, предоставящи обществени услуги, регулираните предприятия и всички структури, които управляват публичен ресурс или осъществяват дейност с висока обществена значимост.

Вътрешният одит допринася за изграждането на доверие чрез независима оценка на прозрачността, законосъобразността, отчетността, етичната среда и надеждността на процесите за вземане на решения.

В публичния сектор този принос може да се изразява в оценка на прозрачността при възлагане на обществени поръчки, управлението на публични

средства, предотвратяването на конфликти на интереси и отчетността пред гражданите. В здравеопазването е свързан с безопасността на пациентите, защитата на медицинската информация, финансовата дисциплина и отговорното използване на ограничените ресурси. В енергетиката и газификацията той се проявява чрез оценка на механизмите за безопасност, устойчивостта на доставките, управлението на критична инфраструктура и спазването на регулаторните изисквания.

Общото между тези примери е, че вътрешният одит не защитава само интереса на конкретната организация. Той подпомага запазването на доверието на потребителите, пациентите, гражданите, партньорите, регулаторите и обществото като цяло.

5. УПРАВЛЕНИЕТО, РИСКЪТ И КОНТРОЛЪТ СЕ РАЗГЛЕЖДАТ КАТО ЕДИННА СИСТЕМА

Новите стандарти подчертават, че управлението, управлението на риска и вътрешният контрол не следва да се разглеждат като самостоятелни и несвързани елементи.

Управлението определя целите, отговорностите и механизмите за вземане на решения. Управлението на риска идентифицира и оценява факторите, които могат да възпрепятстват постигането на тези цели. Вътрешният контрол осигурява конкретните механизми за предотвратяване, откриване и ограничаване на неблагоприятни събития.

Задачата на вътрешния одит е да оцени доколко

тези три компонента функционират съгласувано, дали рисковете са правилно разпознати и приоритизирани и дали контролните механизми са адекватни на реалната среда.

Например при инвестиционен проект вътрешният одит не би следвало да разглежда отделно решение за инвестиция, рисковете от забавяне и контрола върху разходите. Той трябва да оцени дали управлението е взело информирано решение, дали рисковете са анализирани и наблюдавани и дали са въведени достатъчни механизми за контрол на сроковете, бюджета, качеството и договорните отношения.

6. ПО-ГОЛЯМО ЗНАЧЕНИЕ НА ТЕХНОЛОГИИТЕ, ДАННИТЕ И ИНФОРМАЦИОННАТА СИГУРНОСТ

Съвременната организационна среда е все по-зависима от информационни системи, електронни регистри, автоматизирани процеси, обмен на данни и дигитални комуникации. Поради това вътрешният одит следва да развива капацитет за разбиране и оценка на технологичните рискове, надеждността на данните и адекватността на контролните механизми в цифрова среда.

Това не означава, че всеки вътрешен одитор трябва да бъде технически специалист по информационни технологии или киберсигурност. Означава обаче, че одитната функция трябва да може да идентифицира значимите дигитални рискове, да използва данни и аналитични инструменти при изпълнение на одитите и при необходимост да привлича специализирана експертиза.

В дружество за газификация или енергийни услуги

фокусът би могъл да бъде върху защитата на системите за диспечериране и мониторинг, сигурността на данните от измервателни устройства, контрола върху достъпа до технически системи, архивирането на информация и възможността за продължаване на дейността при киберинцидент или техническа авария. В лечебно заведение това може да включва надеждността на болничните информационни системи, защитата на медицинската документация, управлението на достъпа до лични данни и непрекъсваемостта на критичните процеси.

Във всички организации данните все по-често са не само източник на информация, но и стратегически ресурс. Поради това вътрешният одит трябва да оценява не само защитата на данните, но и тяхната точност, пълнота, своевременност и използваемост при вземането на управленски решения.

7. ПОВИШЕНИ ОЧАКВАНИЯ КЪМ КАЧЕСТВОТО И НЕПРЕКЪСНАТОТО ПОДОБРЕНИЕ

Качеството на вътрешния одит не се измерва само чрез наличието на одитни доклади, планове и работни документи. То се проявява в способността на одитната функция да планира риск-базирано, да формулира обосновани заключения, да комуникира ясно, да проследява изпълнението на препоръките и да доказва своя принос за подобряване на организацията.

Новите стандарти поставят по-ясен акцент върху качеството като постоянен управленски процес.

Това включва вътрешни оценки, наблюдение на изпълнението на дейността, измерване на резултатите, самооценка, външна оценка и системно приемане на действия за подобрене.

По този начин вътрешният одит следва да доказва не само че съществува като организационна структура, а че изпълнява своята роля компетентно, независимо, своевременно и с реална полза за организацията.



8. ТЕМАТИЧНИ ИЗИСКВАНИЯ И ПО-ГОЛЯМА ПОСЛЕДОВАТЕЛНОСТ ПРИ ОДИТА НА ЗНАЧИМИ РИСКОВИ ОБЛАСТИ

Към новата Международна рамка за професионални практики са въведени и тематични изисквания. Те имат за цел да осигурят по-голяма последователност и качество при изпълнение на одитни ангажименти, свързани с определени рискови теми.

Тематичните изисквания не заместват професионалната преценка и риск-базирания подход. Те дават минимална обща основа за това какви аспекти следва да бъдат разгледани, когато вътрешният одит изпълнява ангажимент за увереност по съответната тема.

Показателен пример е тематичното изискване за киберсигурност. При одит на тази област вътрешният одит не би следвало да се ограничава до проверка

дали има приета политика по информационна сигурност. Необходимо е да се оцени дали са определени ясни отговорности, дали рисковете се идентифицират и наблюдават, дали се управлява достъпът до системите, дали има механизми за реакция при инциденти, дали се извършва обучение на служителите и дали организацията може да възстанови дейността си след сериозно нарушение или кибератака.

Такъв подход е приложим както при болнична информационна система, така и при дружество, което управлява критична инфраструктура, предприятие с голям брой клиенти, финансова институция, производствена компания или публична администрация.



Обобщение

Новите Глобални стандарти за вътрешен одит утвърждават вътрешния одит като независима, риск-базирана и ориентирана към стойност функция. Те поставят по-високи очаквания както към одиторите, така и към органите на управление и висшето ръководство, като подчертават значението на етиката, обществен интерес, качеството, технологичната компетентност и непрекъснатото подобрене.

В този смисъл вътрешният одит не е просто механизъм за проверка на съответствието. Той е професионален инструмент за подпомагане на доброто управление, за укрепване на доверието и за своевременно идентифициране на възможности за подобрене в интерес на организацията, нейните заинтересовани страни и обществото.

МОЖЕ ЛИ ЕДИН МАЛЪК ОДИТЕН ЕКИП ДА ПОКРИЕ ГОЛЯМА ОДИТНА ВСЕЛЕНА?

ПРАКТИЧЕСКИ ПОДХОД ПРИ СТРАТЕГИЧЕСКОТО ПЛАНИРАНЕ НА ВЪТРЕШНИЯ ОДИТ В ЛЕЧЕБНО ЗАВЕДЕНИЕ

инж. Валентина Пенчева, PhD



РЕЗЮМЕ

Стратегическото планиране на вътрешния одит в лечебно заведение е сложен процес, при който значителният брой управленски, медицински, финансови, административни и технологични дейности трябва да бъде съобразен с ограничен одитен ресурс. Формалното включване на отделни структурни звена в тригодишния план не е достатъчно, за да осигури разумно и защитимо покритие на рисковете.

Настоящата статия представя практически подход за разработване на риск-базирана одитна стратегия в лечебно заведение. Разгледани са изграждането на одитната вселена, изборът на подходящ модел за определяне на одитируемите единици, оценката и групирането на риска, използването на тематични и хоризонтални одитни ангажименти и обвързването на планираните дейности с ефективния фонд работно време на вътрешните одитори. Основен акцент е несъответствието между мащаба на одитната вселена и действителния капацитет на малкия одитен екип, както и възможностите това ограничение да бъде управлявано и коректно докладвано.

Ключови думи: вътрешен одит, стратегическо планиране, лечебно заведение, одитна вселена, оценка на риска, одитируеми единици, хоризонтален одит, одитен ресурс, ефективен фонд работно време.

1. ВЪВЕДЕНИЕ

Лечебното заведение е организация със сложна структура, разнообразни дейности, висока степен на нормативна регламентация и значителна обществена отговорност. В него едновременно протичат медицински, диагностични, финансови, административни, логистични, информационни и управленски процеси. Част от тях са пряко свързани с живота и безопасността на пациентите, други – с финансовата устойчивост, законнообразното разходване на средствата, защитата на информацията, управлението на човешките ресурси и репутацията на организацията.

Тази специфика поставя пред вътрешния одит въпроса как да предоставя достатъчна увереност относно управлението, риска и контрола, когато одитната вселена е значително по-голяма от капацитета на одитния екип.

Практическият проблем може да бъде формулиран по следния начин: Как вътрешният одит да осигури разумно покритие на съществените рискове в лечебно заведение, когато одитируемите области са многобройни, голяма част от тях са оценени като критични или високорискови, а човешкият ресурс е ограничен?

Отговорът не се съдържа единствено в увеличаването броя на планираните ангажменти. Прекомерно амбициозният план, който не е съобразен с реално наличните човекодни, създава риск от неизпълнение, формално приключване на ангажиментите, недостатъчна дълбочина на проверките или компромис с качеството на одитната работа.

Поради това стратегическият план следва да изпълнява ролята на свързващо звено между:

- ▶ целите и приоритетите на организацията;
- ▶ рисковия профил на дейността;
- ▶ одитната вселена;
- ▶ стратегическите цели на вътрешния одит;
- ▶ годишните одитни ангажменти;
- ▶ наличния човешки, времеви и експертен ресурс.

При разработването на тригодишния стратегически план още първоначалното съпоставяне между рисковите единици и наличния ресурс показва, че водещият въпрос не е броят на формално планираните ангажменти, а реално постижимото покритие с необходимата дълбочина и качество. Ето защо стратегическото планиране не трябва да се разбира като еднократно административно действие. То е непрекъснат процес, в рамките на който одитната вселена и рисковата оценка

се актуализират при промени в целите, организационната структура, нормативните изисквания, информационните системи, финансовата среда и ресурсното обезпечаване.

2. СПЕЦИФИКА НА ВЪТРЕШНИЯ ОДИТ В ЛЕЧЕБНО ЗАВЕДЕНИЕ

2.1. Многообразие на одитируемите области

В лечебното заведение одитната вселена не може да бъде ограничена до клиники, отделения, лаборатории и административни звена. Обект на вътрешен одит са и процеси, които преминават през няколко структури и свързват медицинската дейност с финансовото, кадровото, информационното и техническото осигуряване. Едно звено може да участва в няколко процеса, а един процес да се изпълнява от множество звена. Поради това организационната структура сама по себе си не дава пълна картина на рисковете.

В практическата работа най-често се обособяват следните групи одитируеми области:

- ▶ прием, регистрация, идентификация и изписване на пациентите;
- ▶ диагностично-лечебна и оперативна дейност;
- ▶ лекарствено осигуряване и управление на медицински изделия и консумативи;
- ▶ отчитане на медицинската дейност и взаимоотношения с регулаторни органи, НЗОК и други институции, свързани със заплащането на дейността;
- ▶ управление на човешките ресурси, работното време и квалификацията;
- ▶ финансово управление, предварителен контрол, обществени поръчки и договори;
- ▶ информационни системи, информационна сигурност и защита на личните данни;
- ▶ управление на собствеността, техническата инфраструктура, проектната и научната дейност.

Това групиране не означава, че всяка посочена област задължително е самостоятелна одитируема единица. То служи като проверка за пълнота и като отправна точка при определянето на процесите и структурите, които следва да бъдат включени в одитната вселена.

2.2. Граници на вътрешния одит в медицинската дейност

Основно значение има разграничението, че вътрешният одит не оценява клинични решения, избора на терапия или професионалната медицинска експер-

тита. Негов предмет е средата, в която медицинската преценка се упражнява: разпределението на правомощията, организацията и документирането на дейността, надеждността на информацията, функционирането на контролите и управлението на ресурсите и рисковете.

Това разграничение е съществено. Одиторът може да изследва дали правилата са актуални, дали действията са проследими и дали са създадени контролни механизми за безопасност и отчетност, без да навлиза в медицинската целесъобразност на конкретно решение.

2.3. Граници на вътрешния одит при технологична и ИТ зависимост

В лечебното заведение значителна част от дейностите зависят от информационни системи, медицинска апаратура, електронен обмен на данни и надеждност на съхраняваната информация. Поради това технологичната и ИТ зависимост е обосновано включена като рисков фактор при оценката на одитируемите области. В същото време следва ясно да се разграничи, че вътрешният одит не извършва техническа експертиза на информационните системи, медицинската апаратура, мрежовата инфраструктура или киберсигурността, когато не разполага със специализиран ИТ капацитет. Неговият предмет е управленската и контролна среда около използването на технологиите: наличие на правила, разпределение на отговорности, права за достъп, проследимост на действията, надеждност на данните, резервиране на информацията, управление на промени, докладване на инциденти и взаимодействие с външни доставчици.

Това означава, че при оценката на технологичната и ИТ зависимост вътрешният одит може да идентифицира и докладва рискове, свързани с управлението, контрола и отчетността, но не следва да замества специализираната техническа оценка. При необходимост от задълбочена проверка на информационна сигурност, техническа инфраструктура или медицинска апаратура се предвижда участие на компетентни специалисти или използване на външна експертиза.

2.4. Комбинирано въздействие на рисковете

Особеност на лечебното заведение е, че слабост в един процес може едновременно да има медицински, финансови, регулаторни, информационни и репутационни последици. Например недостатъчният контрол върху лекарственото управление може да засегне безопасността на пациента, стойността и наличността на запасите, счетоводното отчитане, спазването на нормативните изисквания и проследимостта на използваните продукти.

По сходен начин прекъсване или компрометиране на

информационна система може да засегне медицинската документация, личните данни, финансовите процеси и непрекъсваемостта на дейността. Затова при планирането не е достатъчно да се оцени само вероятността на риска, необходимо е да се отчете и неговото комбинирано въздействие върху целите на организацията.

3. ОДИТНАТА ВСЕЛЕНА КАТО ОСНОВА НА СТРАТЕГИЧЕСКОТО ПЛАНИРАНЕ

3.1. Същност и предназначение

От теорията е известно, че одитната вселена представлява структурирана съвкупност от всички процеси, дейности, функции, организационни звена, системи, програми, проекти и други области, които могат да бъдат обект на вътрешен одит.

Нейното предназначение не е просто да даде изчерпателен списък на структурите в организацията. Тя трябва да създаде логична и защитима основа за:

- ▶ идентифициране на рисковете;
- ▶ оценяване на одитируемите единици;
- ▶ определяне на одитните приоритети;
- ▶ разработване на стратегическия план;
- ▶ изготвяне на годишните планове;
- ▶ проследяване на одитното покритие;
- ▶ установяване на области, които продължително време не са били одитирани.

Ето защо се наложи да разработим методика за определяне на одитната вселена. Съгласно методиката тя обхваща всички дейности и процеси, които имат съществено влияние върху медицинската, финансовата, административната и управленската дейност, включително области със значим финансов ефект, влияние върху безопасността на пациентите, нормативна значимост или висок оперативен, технологичен, информационен и репутационен риск.

3.2. Организационно звено и одитируема единица

Едно от важните методологични решения е разграничението между „организационно звено“ и „одитируема единица“. Организационното звено е елемент на официалната структура – клиника, отделение, лаборатория, отдел, сектор или друга структурна единица. Одитируемата единица е функционално понятие. Тя може да бъде: организационно звено, процес, дейност, функция, информационна система, проект или програма, външно възложена дейност, механизъм за управление и контрол, система за управление на риска, хоризон-

тална област, която преминава през няколко структури. Разграничението е важно, защото организационната структура показва кой изпълнява дейността, но не винаги показва как протича процесът, къде възникват рисковете и кои контролни механизми свързват отделните участници.

Например процесът по управление на лекарствата може да обхваща болничната аптека, медицинските структури, финансово-счетоводната дейност, обществените поръчки, складовото стопанство и информационните системи. Одитирането само на едно от тези звена не предоставя достатъчна увереност за целия процес.

3.3. Възможни модели за изграждане на одитната вселена

При разработването на одитната вселена приложихме три основни подхода.

Модел по организационна структура. При този подход всяко структурно звено се разглежда като отделна одитируема единица. Предимствата му са свързани с:

- ▶ лесното съпоставяне с организационната структура;
- ▶ ясно определеното ръководство на всяка единица;
- ▶ по-лесното разграничаване на отговорностите;
- ▶ удобството при планиране на ангажменти по звена.

Същевременно този модел има съществени ограничения. Той може да раздружи взаимосвързани процеси и да насочи вниманието към структурата, а не към съществуващия риск. Освен това създава опасност един и същ процес да бъде изследван частично в няколко различни ангажмента, без да бъде оценен цялостно.

Организационният модел е удобен, когато отговорностите са ясно разпределени и управлението е силно структурирано по звена. Той обаче може да доведе до повторно одитиране на един и същ процес в различни структури или до пропускане на рискове, които възникват именно при взаимодействието между тях.

Процесен модел. При този подход одитируемите единици се формират въз основа на управленските, основните и подпомагащите процеси. *Управленските процеси* обхващат планирането, решенията, отчетността, риска и контрола; *основните* следват жизнения цикъл на пациент, т.е. медицинската и диагностично-лечебната дейност; *подпомагащите* осигуряват необходимите

финансови, кадрови, правни, информационни и материални ресурси. Този модел е по-близък до риск-базираното планиране, защото позволява да се проследят:

- ▶ началото и краят на процеса;
- ▶ участващите структури;
- ▶ информационните потоци;
- ▶ разпределението на отговорностите;
- ▶ ключовите рискове;
- ▶ контролните точки;
- ▶ взаимозависимостите с други процеси.

Неговото прилагане изисква по-задълбочено разбиране за организацията и по-висока степен на процесна зрялост. Практическото му ограничение е, че не всички организации разполагат с формално описани процеси, а отговорността за един процес може да бъде разпределена между няколко ръководители.

Хибриден модел. Практически най-подходящ за лечебното заведение се оказва хибридният модел, при който процесите и организационните звена се разглеждат във взаимна връзка. Логиката може да бъде представена така: структура → процес → одитируема единица → риск.

При този модел:

- ▶ на първо ниво се определят управленските, основните и подпомагащите процеси;
- ▶ на второ ниво се идентифицират структурите, които участват в изпълнението им;
- ▶ на трето ниво се обособяват конкретните одитируеми единици;
- ▶ на четвърто ниво се идентифицират и оценяват рисковете.

Този подход съчетава яснотата на организационния модел с риск-ориентирания характер на процесния модел. В разработената методика е възприет именно хибридният подход, като е отчетено и обстоятелството, че една структура може да участва в повече от един процес, без това да представлява методологично противоречие, когато ролята ѝ е различна в отделните процеси.

Практическият ефект от този избор се вижда при процеси като например лекарственото управление. Ако аптеката се разглежда изолирано като организационно звено, извън анализа могат да останат планирането на потребностите, обществените поръчки, приемането и складовото отчитане, отпускането към медицинските

структури, финансовото отчитане и правата за достъп в използваните системи. Процесният поглед свързва тези дейности, а организационният позволява ясно да се определят отговорните лица и звена.

4. ПРАКТИЧЕСКИ ЕТАПИ ЗА РАЗРАБОТВАНЕ НА ОДИТНАТА ВСЕЛЕНА

Изграждането на одитната вселена следва да се извършва по предварително определена и документирана последователност. Целта не е само да се състави списък, а да се получи работещ модел на организацията, който позволява проследяване на връзките между цели, процеси, структури, рискове и контролни механизми.

4.1. Разбиране на организацията и нейните процеси

Началната стъпка е проучването на устройствените документи, организационната структура, бизнес плана и стратегическите цели, вътрешните правила, финансовите и управленските отчети, договорите, информационните системи и резултатите от предходни одити и проверки. Документалният преглед следва да бъде допълнен с разговори с ръководството и отговорните длъжностни лица, за да се установи как процесите действително функционират.

Особено значение имат бизнес планът и управленските цели, защото одитната вселена следва да бъде свързана не само с текущата структура, но и с посоката на развитие на лечебното заведение. Ако например се предвижда внедряване на нова информационна система, разширяване на медицинска дейност или значителна инвестиция, тези промени трябва да бъдат отразени още при стратегическото планиране.

Полезни източници са също регистрите на рисковете, докладите на външни контролни органи, данните за жалби и сигнали, инциденти, просрочени вземания и задължения, отклонения от бюджетите и неизпълнени препоръки. Те насочват вниманието към области, в които формално установените правила може да не съответстват на действителното функциониране на контролите.

4.2. Обособяване на одитируемите единици

За всеки процес се идентифицират звената, които го инициират, изпълняват, контролират и отчитат. След това се определя подходящото ниво на одитируемата единица. Твърде общата единица може да обединява несъпоставими дейности и рискове, а прекомерното раздробяване води до необосновано голяма одитна вселена и прави практическото ѝ покритие невъзможно. Подходящото ниво трябва да позволява самостоятелно идентифициране на риска, определяне на отговорно



ръководство, планиране на реалистичен одитен обхват, проследяване на предходни проверки и оценяване на необходимия ресурс. Подпроцесите могат да бъдат използвани при планиране на конкретен ангажимент, без непременно всички да се превръщат в самостоятелни единици в основния регистър.

В конкретната работа това означаваше някои първоначално формулирани единици да бъдат обединени, когато рисковете и контролите им бяха неразделно свързани, а други да бъдат разделени, когато в една обща област се съдържаха несъпоставими дейности. Критерият не беше броят на звената, а възможността за ясно определен одитен предмет, отговорност и необходим ресурс.

4.3. Проверка за пълнота и актуализиране

След съставяне на първоначалния списък се проверява дали са включени всички съществени структури и процеси, стратегически проекти, информационни системи, външно възложени дейности, механизми за управление на риска и области с влияние върху пациентската безопасност или значителен финансов ефект. Особено внимание изискват хоризонталните области, които често остават извън модел, изграден само по организационната структура.

При проверката за пълнота могат да се използват няколко практически въпроса: има ли значими финансови потоци, които не са свързани с конкретна единица; съществуват ли критични информационни системи извън обхвата; има ли външно възложени дейности без ясно определен контрол; кои процеси имат пряко влияние върху пациента; и кои области не са били обект на одит или друга независима проверка продължително време?

Тази проверка е особено важна при първоначалното изграждане на одитната вселена, защото липсата на предходна систематизирана информация може да доведе до неволно изключване на нови, хоризонтални или технологични рискове.

За всяка единица е полезно да се документира връзката с целите, участващите структури, ключовите рискове, контролите, използваните системи и резултатите от предходни одити. Одитната вселена не е статичен документ; тя трябва да се актуализира при организационни, нормативни, технологични и други съществени промени.

5. ОЦЕНКА И КЛАСИФИЦИРАНЕ НА РИСКА

5.1. Роля и обхват на оценката

Разработването на одитната вселена показва какво може да бъде одитирано, но не определя самостоятелно какво следва да бъде одитирано с предимство. Оценката на риска създава съпоставимост между различни по характер единици, подпомага определянето на приоритетите и обосновава вида, честотата и обхвата на одитната работа.

В разглеждания практически модел са оценени всички единици от одитната вселена, а не само предварително възприеманите като съществени. Това осигурява проследим рисков профил, позволява сравнение и предотвратява предварително изключване на области само по субективна преценка. Нискорискова единица също трябва да има начална оценка, защото при нормативна, организационна или технологична промяна нейният приоритет може да се повиши.

5.2. Рискови фактори

За да бъдат приложими към управленски, основни (медицински) и подпомагащи процеси, рисковите фактори трябва да бъдат достатъчно общи за сравнение, но и достатъчно конкретни, за да отразят особеностите на лечебното заведение. В разработения модел са използвани следните седем рискови фактори:

- ▶ *Технологична и IT зависимост* – отчита зависимостта на дейността от информационни системи, медицинска апаратура, технологии и надеждността на данните.
- ▶ *Договорен риск* – свързан е със значимостта на договорните отношения и възможните последици при неизпълнение, забавяне или нарушение.
- ▶ *Регулаторен риск* – отразява степента на нормативна регламентация и риска от санкции, предписания, финансови корекции или други неблагоприятни последици.
- ▶ *Вътрешен контрол* – оценява надеждността на контролната среда, разпределението на отговорностите, проследимостта на действията и вероятността от грешки или отклонения.

5.3. Оценъчна скала, тегла и рисков индекс

За оценка на факторите сме използвали скала от 1 до 5, като за всяка стойност предварително сме определили съдържание. Стойност 0 не следва да се използва за минимален риск, защото може да означава липса на информация, неприложим фактор или неизвършена оценка. Когато рискът е минимален, се използва най-ниската стойност от скалата – 1; когато факторът не е приложим, това се отбелязва отделно.

За да се ограничи различното тълкуване, към всяка степен сме определили критерии. Например при регулаторния риск оценка 1 може да се постави при относително устойчива среда и ограничени последици от отделно несъответствие, а оценка 5 – когато дейността е силно регулирана и нарушението може да доведе до тежки санкции, прекъсване на дейността или риск за пациента. Аналогични критерии са необходими и за останалите фактори.

Полезна контролна стъпка е след първоначалното оценяване да се прегледа общото разпределение на единиците по рискови групи. Ако почти всички единици попадат в една и съща група, това може да показва недостатъчно разграничени критерии, неподходящи тегла или прекалено общо оценяване. Целта не е резултатите да бъдат изкуствено разпределени, а моделът да различава съществените нива на риск.

Оценяването е добре да бъде обсъдено и с ръководители на ключови процеси, без това да прехвърля върху тях отговорността за окончателния резултат. Техните обяснения могат да допълнят информацията за настъпили промени, действието на контролите и предстоящи инициативи, но вътрешният одитор запазва независимата професионална преценка и документира основанията за нея.

- ▶ *Репутационен риск и влияние върху пациента* – отчита възможните последици за пациентите, общественото доверие и репутацията на лечебното заведение.
- ▶ *Финансов риск* – отразява значимостта на управляваните финансови средства, активи, разходи и възможните финансови загуби.
- ▶ *Стратегически риск* – оценява значението на съответната област за постигане на целите, устойчивостта и развитието на лечебното заведение.

При първоначално разработване на модела е полезно да се извърши и пробно оценяване на няколко различни по характер единици. Така могат да се установят неясни критерии, фактори с прекалено голямо или малко влияние и формули, които не дават очакваната съпоставимост. Корекциите трябва да бъдат направени преди окончателното оценяване на цялата одитна вселена.

От одиторската практика е известно, че не всички фактори имат еднакво значение. Ето защо могат да бъдат използвани предварително определени тегла с общ сбор 100%. Рисковият индекс се формира чрез умножаване на оценката по всеки фактор с неговото тегло и сумиране на претеглените резултати.

След изчисляването разпределихме единиците в рискови групи – критичен, висок, среден, нисък и незначителен риск. Границите улесняват приоритизирането, но трябва да се използват внимателно. Например единици с индекси 3,9 и 4,0 попадат в различни групи, въпреки че числовата разлика е минимална.

Поради това при определянето на приоритета се отчитат и времето от последния одит, резултатите от предходни проверки, неизпълнените препоръки, настъпилите промени, инцидентите, изискванията на ръководството и наличната компетентност в одитния екип. Две единици с еднакъв индекс могат основателно да бъдат планирани в различни години или с различен вид ангажимент.

5.4. Професионална преценка и „критичен сигнал“

Един от недостатъците на претеглената средна оценка е, че много висока стойност по отделен фактор може да бъде компенсирана от по-ниски оценки по останалите. Например процес с ограничен финансов риск, но с пряко влияние върху пациентската безопасност, може да остане под границата за критичен риск.

Затова е целесъобразно да се предвиди правило за „критичен сигнал“. Максимална оценка по фактор като безопасност на пациента, прекъсване на критична медицинска дейност, значима информационна заплаха или риск от загуба на разрешение следва да води до допълнителна професионална преценка независимо от общия индекс.

5.5. Документиране и ограничения на модела

Към числовите оценки трябва да бъдат посочени кратки аргументи и източници: нормативни изисквания, финансови и статистически данни, отчети за дейността, резултати от външни проверки и предходни одити, информация за инциденти, жалби и сигнали, кадрови или технологични промени и интервюта с отговорни-

те лица. Така при следваща актуализация може да се установи защо оценката се е променила.

Добрата практика е кратката аргументация да бъде записана непосредствено до оценката. Например висока оценка за регулаторен риск може да бъде подкрепена с информация за нови изисквания, констатиран несъответствия или предстояща външна проверка. Така при следващото годишно актуализиране е ясно дали промяната в стойността се дължи на реално изменение на риска или само на различна субективна преценка.

Всеки модел съдържа субективност и е зависим от качеството на първичната информация. Числовата форма може да създаде привидност за точност, поради което рисковият индекс трябва да се разглежда като структуриран инструмент за вземане на решения, а не като автоматичен заместител на професионалната преценка.

6. ОТ ОЦЕНКАТА НА РИСКА КЪМ ТРИГОДИШНИЯ ПЛАН

Рисковата група не е равнозначна на самостоятелен одитен ангажимент. При голяма одитна вселена и малък екип механичното превръщане на всяка критична или високорискова единица в отделен пълен одит води до неизпълним план. Практическият разчет ясно показва това ограничение. Ако за един ангажимент по критичен риск се предвидят примерно до 60 човекодни, само десет критични единици биха изисквали приблизително 600 човекодни. Към тях трябва да се прибавят високорисковите области, планирането, докладването, проследяването на препоръките, обучението, качеството и извънплановата работа.

Затова критичните рискове трябва да получават системно внимание, но не непременно ежегоден пълен одит. Покритието може да бъде разпределено за целия период чрез пълен, тематичен или хоризонтален ангажимент, ограничен преглед, проследяване на препоръки или използване на надеждни резултати от други проверки. Важно е да се документира каква част от риска е обхваната, каква увереност е получена и кои елементи остават непроверени.

Приоритизирането не се изчерпва с подреждане по индекс. От значение са стратегическата значимост на процеса, прякото отражение върху пациента, размерът на управляваните ресурси, новите нормативни изисквания, внедряването на системи, данните за нарушения и инциденти, резултатите от външни проверки и периодът от последното одитно покритие.

Това позволява и по-гъвкаво планиране. Единица с висок риск може да бъде включена в по-широк тематич-

чен ангажимент, а критична област с вече извършена надеждна външна проверка може временно да получи ограничен преглед или проследяване, ако професионалната преценка показва, че остатъчният риск е приемлив.

Средният и ниският риск също не означават трайно изключване. Такива единици могат да бъдат включени при съществена промяна, възникнал инцидент, връзка с високорисков процес, продължителен период без одит или наличие на свободен ресурс. Рисковият профил се актуализира ежегодно, за да може стратегическият план да бъде устойчив като посока, но гъвкав по отношение на конкретните приоритети.

При тригодишното разпределение е важно да се избегне и обратният риск – всички ресурси да бъдат насочени само към най-високите оценки, така че други области да останат без независимо внимание за твърде дълъг период. Затова освен рисковата група може да се приложи и ротационният принцип, времето от последния одит и възможността дадена единица да бъде включена като част от по-широк ангажимент.

В стратегическия план е полезно за всяка планирана тема да се посочи кои критични или високорискови единици получават пълно или частично покритие. Това създава видима връзка между оценката на риска и избраните ангажименти и позволява при ежегодното актуализиране да се установи кои области продължават да остават без независимо внимание.

Подобна проследимост е важна и при промяна на плана. Когато ангажимент бъде отложен поради извънпланова задача, трябва да се види какъв риск остава непокрит и дали той може да бъде управляван чрез друг вид работа или трябва да бъде прехвърлен с приоритет към следващата година.

7. ТЕМАТИЧНИ И ХОРИЗОНТАЛНИ ОДИТНИ АНГАЖИМЕНТИ

7.1. Същност и основания за групиране

Тематичният ангажимент е насочен към конкретна област, риск или група сходни дейности, а хоризонталният изследва един и същ процес, риск или контролен механизъм в няколко структури. Те позволяват ограничен брой ангажименти да обхванат взаимосвързани рискове, без да се планира отделен одит за всяко звено.

Групирането трябва да се основава на общ процес, сходен риск, еднакви вътрешни правила, обща информационна система, поток на средства, документи или данни или общ собственик на процеса. Например звената, които участват в планирането, възлагането, изпълнението и плащането по договори, могат да

бъдат включени в общ ангажимент по управление на договорния процес.

7.2. Практически пример за хоризонтален ангажимент

Хоризонтален ангажимент по управление на достъпа до болнични и административни информационни системи може да обхване ИТ звеното, човешките ресурси, финансово-счетоводната структура, регистратурата, аптеката и избрани медицински звена. Одитът може да провери предоставянето и прекратяването на достъп, съответствието между длъжност и права, периодичния преглед на потребителите, привилегированите профили и действията при кадрови промени.

Този подход позволява да се установи дали общите правила се прилагат последователно и дали слабостите са единични или системни. Той може да доведе до препоръки към собственика на процеса или ръководството, а не само към отделно звено.

Основните предимства са възможността да се откриват системни слабости, да се сравняват практики между



звената и да се формулират препоръки на ниво процес или управление. Когато едно и също несъответствие се наблюдава в няколко структури, причината често е в общите правила, недостатъчната координация или липсата на централен контрол, а не само в действията на отделен ръководител.

7.3. Широко и пълно покритие

Широкото покритие не е равнозначно на пълен одит. Когато един риск е проверен в няколко структури, това не означава, че всички техни дейности са одитирани. В плана и регистъра на одитната вселена следва да се отбелязва дали покритието е пълно, частично, тематично, хоризонтално, консултативно или представлява проследяване на препоръки.

В годишния план трябва да бъдат конкретизирани темата, основният риск, включените процеси и структури, очакваният обхват, необходимите човекодни и видът на покритието. Това позволява по-късно да се проследи не само дали единицата е била включена в ангажимент, а каква част от нейния рисков профил действително е проверена.

При хоризонталните ангажименти може да се използва риск-базирана извадка или ротационен принцип. Например всички клиники могат да бъдат включени в предварителен анализ на показатели, а детайлно тестване да се извърши само в звената с най-висок риск, отклонения или обем на дейността. Критериите за извадката и ограниченията на резултатите трябва да бъдат ясно документираны.

Извадката трябва да бъде съобразена с целта на ангажимента. Когато се проверява последователното прилагане на общо правило, в нея следва да има структури с различен профил – например големи и малки звена, медицински и административни участници, звена с различен обем на дейност или с установени отклонения. Това увеличава възможността да се разграничат единичните слабости от системните проблеми.

Одитният доклад трябва ясно да посочва границите на направените изводи. Констатация, установена в избрани звена, не може автоматично да бъде отнесена към цялата организация, ако извадката и използваните доказателства не позволяват това. Коректното описание на обхвата е част от надеждността на одитната работа.

Тематичният и хоризонталният подход е средство за оптимизиране, а не за прикриване на ограниченията. При прекалено широк обхват се увеличава рискът от повърхностно изследване, общи констатации и недостатъчна доказателствена стойност. След определена граница разширяването на обхвата започва да намалява дълбочината и надеждността на одита.

8. РЕСУРСНОТО ОГРАНИЧЕНИЕ КАТО ЧАСТ ОТ ОДИТНИЯ РИСК

8.1. Реалистичното планиране започва от наличния ресурс

Риск-базираното планиране не приключва с определянето на критичните и високорисковите области. Следва да се изчисли наличният ефективен фонд, да се разпредели по видове дейности, да се определят необходимите човекодни и да се установи какъв риск остава непокрит.

На практика често първо се съставя списък на желаните ангажименти, а едва след това се проверява

дали има достатъчно време. Така се получава план, който изглежда убедително като обхват, но е неизпълним. По-правилно е ресурсът да бъде ограничението, в рамките на което се определят броят, видът и дълбочината на ангажиментите.

Логичната последователност е: първо да се определи индивидуалният фонд на всеки одитор, след това времето да се разпредели между одитни ангажименти, планиране, проследяване, обучение, качество и административни дейности, и едва тогава да се избере реалистичният брой ангажименти. Остатъкът между желаното и възможното покритие представлява непокрит риск, който трябва да бъде видим в плана.

8.2. Щатна численост и действителен капацитет

Утвърдената численост не винаги е равнозначна на реално наличния ресурс. В разглеждания случай звеното включва ръководител на вътрешния одит и вътрешен одитор, който работи на половин работен ден. Формално са налице две щатни бройки, но от гледна точка на работното време капацитетът е приблизително 1,5 еквивалента на пълно работно време.

И тази стойност не отразява напълно времето за непосредствени одитни ангажименти. Ръководителят изпълнява постоянни функции по стратегическо и годишно планиране, оценка на риска, надзор, качество, докладване, методология, проследяване на препоръките и административно управление. Тези функции съществуват независимо от размера на екипа и при малка численост заемат по-голям относителен дял.

Непълното работно време има и организационни последствия, които не се изчерпват с аритметичното намаляване на човекодните. Част от одитната работа изисква участие в срещи в определени часове, съвместни проверки, бърза реакция при възникнали въпроси и непрекъснато проследяване на сложни процеси. Разпокъсването на работния ден може да увеличи времето за координация и да намали оперативната гъвкавост.

Поради това при стратегическото планиране е необходимо да се прави разграничение между формално утвърдена численост, еквивалент на пълно работно време и реално наличен капацитет за изпълнение на одитни ангажименти.

8.3. Ефективен фонд работно време

Ефективният фонд работно време е времето, с което одиторът реално разполага през годината след приспадане на отпуските и другите периоди, през които не

е на разположение. При непълно работно време един календарен работен ден не е равен на един пълен човекоден. Например 200 ефективни дни при четири-часов работен ден представляват 100 еквивалентни човекодни.

Когато членовете на екипа имат различно работно време, отпуски или периоди на заетост, фондът следва да се изчисли индивидуално за всеки от тях и едва след това да се обедини. Простото използване на средна стойност може да прикрие съществени различия в реалния принос.

Практически полезен инструмент е ежедневното отчитане на времето по основни видове дейности в специално изготвена електронна таблица. За целта времето може да бъде разпределено по категории като ангажименти за увереност, консултативни задачи, проследяване на препоръки, планиране и оценка на риска, методологична работа, обучение и административни дейности.

Таблицата не трябва да се превръща в самоцелна административна отчетност. Нейната стойност е в натрупването на фактически данни, които показват колко време действително изискват различните дейности, кои задачи системно се подценяват и къде възникват отклонения от плана.

Анализът на отчетеното време може да покаже различия между планираната и действителната продължителност на отделните етапи на ангажимента. Ако например предварителното проучване, събирането на документи или обсъждането на проекта на доклад системно изискват повече време, това следва да бъде отразено в бъдещите разчети, вместо отклонението да се приема като еднократно.

При изчисляване на условията необходим брой одитори трябва да се използват съпоставими величини. Ако в необходимия ресурс са включени всички дейности на звеното, той се сравнява с целия ефективен фонд. Ако се анализират само човекодните за ангажименти, те трябва да се сравняват само с дела от фонда, предназначени за непосредствена одитна работа.

Когато общият необходим ресурс се раздели на ефективния фонд на един пълен зает одитор, получената стойност представлява условен еквивалент, а не автоматично предложение за щат. Тя показва разликата между необходимото и наличното покритие и служи като аргумент при обсъждане на ресурсните решения.

По този начин ресурсното приложение към стратегическия план се превръща в инструмент за управление, а не само в доказателство, че общият брой дни е математически разпределен.

8.4. „Другата одиторска работа“ не е свободен резерв

Към другата одиторска работа се отнасят методологията, изграждането и актуализирането на одитната вселена, годишната оценка на риска, планирането, периодичното и годишното докладване, управлението на качеството, поддържането на досиетата, текущите справки и професионалната координация. Тези дейности не са остатъчни, а задължителна част от функционирането на звеното.

Техният дял е особено значителен през първата година от тригодишния период, когато едновременно се разработват методологията, одитната вселена, оценката на риска, стратегическият план и приложенията, докато продължава изпълнението на текущите ангажименти. В конкретния случай първоначално предвидените дни за този вид работа се оказаха недостатъчни още през първото полугодие. Това показва, че разчетът трябва да се коригира въз основа на фактически отчетеното време, а не да се запазва формално първоначалната стойност.

Когато стратегическият план се разработва след началото на календарната година, първата година не следва да се третира като пълна ресурсна година. Необходимо е да се отчетат вече изразходваните дни, текущите ангажименти, оставащите отпуски и времето за подготовка на следващия годишен план. В противен случай в оставащите месеци могат да бъдат включени задачи, за които календарно няма възможност за изпълнение.

Планът трябва да съдържа и реалистичен резерв за извънпланови задания, сигнали, нормативни промени, външни проверки, непредвидени отсъствия и съществени промени в рисковия профил. План без резерв е уязвим още при първата непредвидена задача.

8.5. Човекодни и календарна продължителност

Човекодният позволява ресурсът на различните служители да бъде представен в обща измерима величина. Необходимите човекодни за ангажимент се определят според сложността на процеса, броя на включените структури, обема на документацията, необходимостта от анализ на данни, броя и вида на тестовете, наличието на предходни одити, опита на екипа и необходимостта от външна експертиза.

Рисковата категория определя приоритета, но не и автоматично продължителността. Две критични единици могат да изискват различен ресурс в зависимост от организацията на процеса, качеството на документацията и броя на участващите звена. Календарната

продължителност също не е равнозначна на човекодните, тъй като един ангажимент може да се изпълнява от различен брой одитори, с прекъсвания и с различно разпределение между изпълнение и надзор. Например ангажимент в ясно структуриран процес с надеждна информационна система и налични предходни работни документи може да бъде изпълнен с по-малък ресурс от ангажимент със същата рискова категория, който обхваща много звена, ръчни операции, непълна документация и сложна нормативна среда. Затова предварителното проучване е необходимо и за реалистичното определяне на човекодните.

8.6. Ресурсният дефицит като непокрит риск

Когато необходимите човекодни надвишават наличния фонд, възниква ресурсен дефицит. Той не трябва да бъде прикриван чрез намаляване на времето под професионално необходимото, прекомерно групиране на несвързани области, формално включване на единици без реално тестване, премахване на времето за планиране и качество или отказ от обучение и резерв.

Ресурсният дефицит означава, че част от съществениите рискове няма да получат желаното одитно покритие. Пред ръководството следва ясно да се представят наличните и необходимите човекодни, разликата между тях, областите, които няма да бъдат покрити, възможните последици и вариантите за управленско решение.

Това съобщаване не трябва да се възприема като отказ от изпълнение, а като част от професионалната отговорност на ръководителя на вътрешния одит. Ръководството трябва да разполага с достатъчно информация, за да реши дали да увеличи ресурса, да промени приоритетите, да приеме остатъчния риск или да осигури друг източник на увереност.

В разглеждания случай именно сравнението между одитната вселена, планираните човекодни и фактическата заетост на втория одитор показва, че работата на половин ден ще бъде съществено ограничение за покриване на високорисковите области. Този извод не произтича от общо усещане за натовареност, а от конкретен ресурсен разчет и от отчетеното време за задължителните професионални дейности.

Така аргументът пред ръководството е по-ясен: въпросът не е дали екипът може да работи по-интензивно, а каква увереност може надеждно да предостави с наличния капацитет. Това поставя дискусията върху управленски избор между ресурс, обхват и приемане на остатъчния риск.

8.7. Възможни управленски решения

Възможните решения включват преминаване на одитора на пълен работен ден, увеличаване на числеността, осигуряване на външна експертиза за специализирани области, преразпределяне на стратегическите приоритети, ограничаване на обхвата на част от ангажиментите, тематично и хоризонтално групиране и многогодишно ротационно покритие.

Всяко решение има различен ефект. Преминаването на пълен работен ден увеличава непрекъснатостта и възможността за съвместни проверки. Външната експертиза е подходяща за специализирани медицински, технически или информационни области, но не замества постоянния вътрешен капацитет. Ограничаването на обхвата може да бъде професионално обосновано, ако оставащите извън проверката рискове са ясно посочени и планирани за последващо покритие.

Изборът е управленска отговорност. Отговорността на ръководителя на вътрешния одит е да представи ясно връзката между ресурса, възможното покритие и остатъчния риск. Когато наличният фонд е недостатъчен, професионално правилното решение не е формално разширяване на плана, а открито докладване на ограничението.

9. ЗАКЛЮЧЕНИЕ

Разработването на одитна вселена, оценката на риска и ресурсното планиране показват, че стратегическият план за вътрешен одит в лечебно заведение не може да бъде само списък от бъдещи ангажименти. Той следва да бъде обоснована управленска рамка, която свързва съществениите рискове, наличния одитен капацитет и реално постижимото покритие.

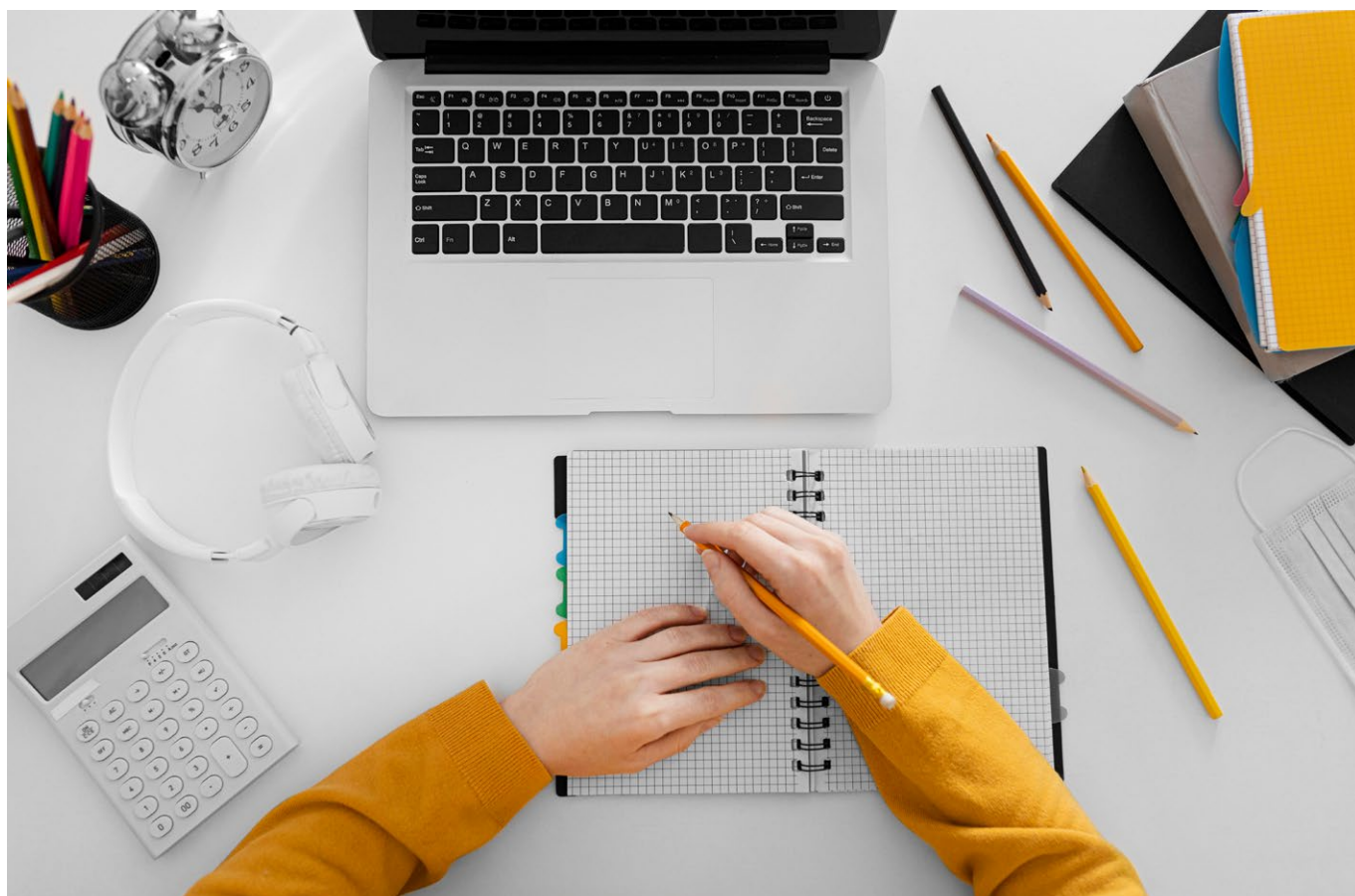
В този смисъл отговорът на въпроса дали един малък одитен екип може да покрие голяма одитна вселена зависи от това какво се разбира под „покритие“. Малкият екип може да осигури професионално обосновано внимание към най-съществениите рискове, когато одитната вселена е ясно структурирана, оценката е съпоставима, а ангажиментите са разпределени многогодишно и ресурсно обезпечени.

Тематичните и хоризонталните ангажименти, риск-базираните извадки и поетапното покритие увеличават ефективността, но не превръщат частичното покритие в пълен одит и не могат неограничено да компенсират недостига на човекодни.

Качественият стратегически план не е планът с най-голям брой ангажименти. Качествен е планът, който показва проследимо кои рискове ще бъдат обхванати, с каква дълбочина, в какъв период и с какъв ресурс, както и кои ограничения и остатъчни рискове следва да бъдат приети или управлявани от ръководството.



СТАНЕТЕ ЧАСТ ОТ СПИСАНИЕ "ВЪТРЕШЕН ОДИТОР", ПУБЛИКУВАЙТЕ **ВАШ** АВТОРСКИ ИЛИ ПРЕВОДЕН МАТЕРИАЛ



Списание „Вътрешен одитор“ е издание на Института на вътрешните одитори в България и се издава от 2004 г. Това е единственото специализирано периодично издание за вътрешен одит, вътрешен контрол, управление на риска и корпоративно управление в България. Читателите на списанието са професионалисти в корпоративния, банковия и застрахователния сектор, както и одитори и експерти от публичния сектор.

В списанието се публикуват авторски статии на водещи български специалисти, преводни статии от сп. „Internal Auditor“, издание на Международния институт на вътрешните одитори, The IIA (www.theiia.org), или други специализирани издания, новини, коментари и информация за предстоящи събития в България, Европа и в света, свързани с одит, контрол и управление на риска.

На страниците на списанието намират място мате-

риали на разнообразна тематика в областта вътрешния одит, външни оценки на качеството на вътрешния одит; противодействие на измамите, ИТ одит и сигурност на ИТ средата, добро корпоративно управление, в т.ч. и управление на човешки ресурси, новости и промени в нормативната уредба, свързана с публичния, застрахователния и банковия сектор, прилагане на рамки за вътрешен контрол и системи за управление, комуникативни умения на вътрешните одитори. Също така, интервюта с успели в професията и с млади ентусиасти, насочили се към нея.

Възползвайте се от възможността да станете сътрудници на списанието, като ни предоставите свой авторски материал по актуални теми в посочените по-горе области. Можете да споделите предварително Вашата идея за тема или направо да ни изпратите вече готов материал. Темата ще бъде разгледана от редакционния съвет на списанието, а главният редактор ще уточни с Вас срока, в който материалът трябва да бъде подготвен. Преди да бъде публикувана, статията ще бъде подробно прегледана и коригирана.

В списание „Вътрешен одитор“ се препечатват и най-интересните статии от международното списа-

ние "Internal Auditor". Ако желаете да преведете такава статия, можете да се свържете с нас, като ще получите от главния редактор материали на разнообразна тематика. В списанието могат да намерят място и преводни материали от други издания, като е задължително предварително да бъдат уредени авторските права и да бъде получено разрешение за препечатване. Авторските статии на български език, както и преводите на специализирани материали се заплащат по утвърдена тарифа.

Препоръчителният обем на статиите е от 3 до 5 страници. Шрифтът, който се използва за определяне на обема, е Arial, размер 10. Статиите се предоставят във формат MS WORD. Ако материалът е по-дълъг от 5 стр. се публикува съобразно възможностите на текущото издание или се разделя и се публикува в поредни броеве.

При проявен интерес от Ваша страна, моля, свържете се директно с главния редактор на списанието или с офиса на ИВОБ на имейл.адрес:

IIABulgaria@mbox.contact.bg

Допълнителна информация към авторите на статии

1. Заглавието на статията трябва да бъде достатъчно информативно относно темата на статията, като съкращения в него не се допускат. След заглавието се посочва името на автора.
2. Снимка на автора в отделен файл.
3. Кратко представяне на автора.
4. Всички източници, които авторът е използвал и цитирал в материала, трябва да бъдат пълно и точно изписани от него в бележка под линия или в списък с бележки в края на статията.
5. В края на статията под наименованието „Използвана литература/Източници...“ от автора задължително се описват пълно и точно всички източници, използвани при изготвянето на материала.
6. Използването на сложна, непопулярна и по-специфична терминология трябва да бъде пояснена от автора в скоби след съответния термин или в бележка под линия. Същите правила се прилагат и при използване на съкращения.
7. Заплащането на материалите е по одобрена от УС на ИВОБ тарифа.

Certified for **Success.**

An IIA certification opens doors & elevates success.



Learn More



The Institute of
Internal Auditors



The Institute of
Internal Auditors



Elevating **Impact**

The IIA empowers internal auditors to foresee potential risks that drive organizational success and enhance value. Elevating impact at every level, the world over, we are The IIA.

Membership | Standards | Certifications | Learning

www.theiia.org