СЪВМЕСТНА РАБОТА НА СИСТЕМИ ЗА УПРАВЛЕНИЕ ПО ISO&ISO/IEC - СТАНДАРТИ СЪС СИСТЕМА ЗА УПРАВЛЕНИЕ НА РИСКА

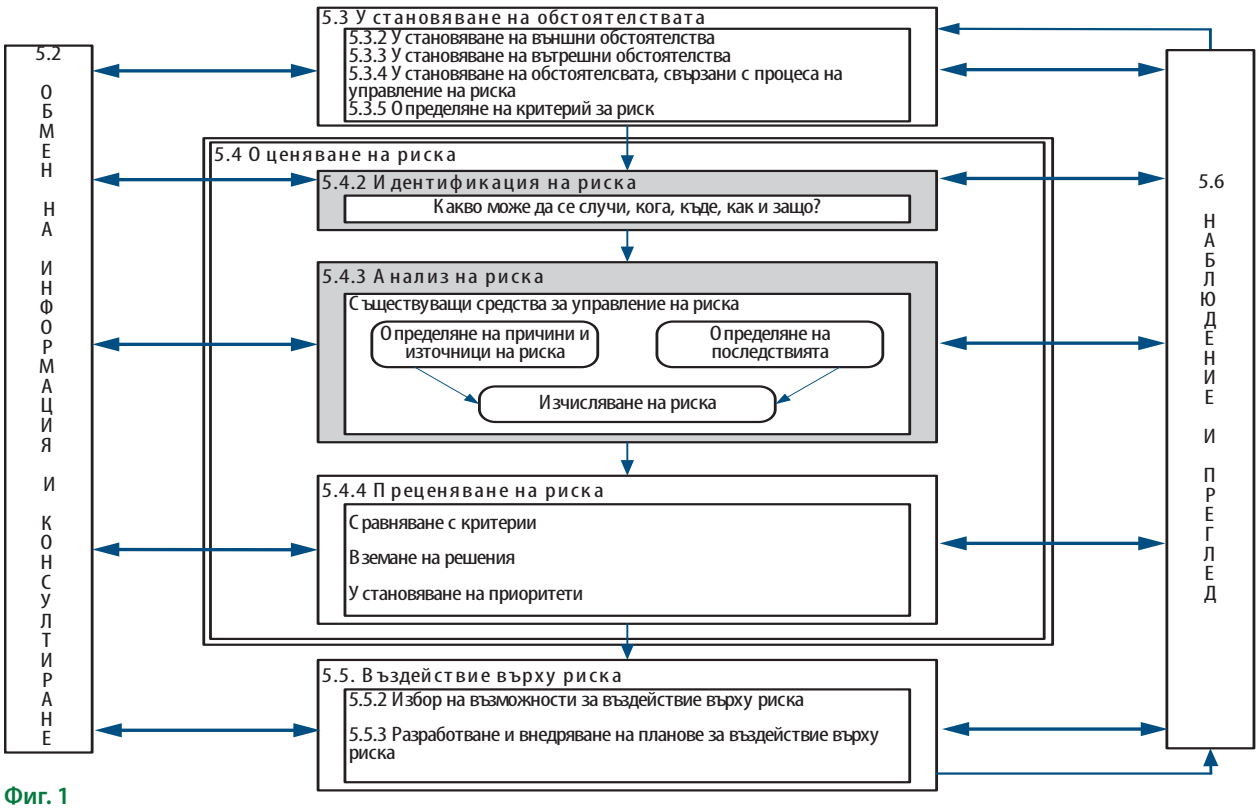
проф. д-р Илия ЦЕНЕВ, СМС - управител на „Практика-О.К." ООД
Димитър БАНТУТОВ - експерт от „Практика-О.К." ООД
д-р инж. Георги ПОПОВ, QEP - University of Central Missouri, USA
инж. Мариана ШИРКОВА, СМС - управител на фондация „Качество 21-ви век"
доц. д-р Пламена ЗЛАТЕВА - БАН, експерт към фондация „Качество 21-ви век"
инж. Недялко ИВАНОВ - консултант към „Екома" ЕООД, аспирант към БАН

Поводът да напишем настоящия материал, в който се показва съвместната работа на двойката стандарти (БДС ISO 31000:2011 „Управление на риска. Принципи и насоки" и БДС ISO 31010:2011 „Управление на риска. Методи за оценяване на риска") и стандарти за системи за управление (ISO 9001:2008, ISO 14001:2004, ISO/IEC 17011:2004, ISO/IEC 17020:1998, ISO/IEC 17021:2011, ISO/IEC 17024:2003, ISO/IEC 17025:2005, BS OHSAS 18001:2007, ISO 22000:2005, ISO 27001:2005, ISO 28000:2007 и други) е проявен интерес от познати и непознати колеги, които бяха прочели публикацията ни в брой 5-6/2011 г. на списание „Машиностроене и електротехника". По този повод ние направихме справка, която показа че стандартите за оценка на риска не са популярни в България. На настоящия етап се откриха три публикации на български език и огромен брой публикации, по тази тема по света. От http://www.mod.bg/bg/doc/programi/20110516_ModelRisk.pdf е показан модел за управление на риска при планиране на отбраната и въоръжените сили. Моделът е създаден от група експерти от Министерство на отбраната и се базира на двата международни станарта по оценка на риска. В http://nslatinski.org има серия от материали за оценка на риска, свързани с националната сигурност, публикувани от доц. д-р Николай Слатински. В тях се дават препоръки за системи за управление на риска в цитираната област, като се прилага методологията на двата международни стандарта. В http://mm-businessconsult.com има информационен материал от г-жа Мая Михайлова за ISO 31000:2009.

КАКВО ПРЕДСТАВЛЯВА ПРОЦЕСА НА ОЦЕНКА НА РИСКА

На фиг. 1 е показан този процес. Обозначените точки на фигурата кореспондират със съответните точки на стандарт БДС ISO 31000:2011. Така показания процес като теория и практика е описан в множество литературни източници. Той не е новост за специалистите в тази област. Включен е в международния стандарт т.е. представлява част от цялостната система за управление на риска. Резюмирано процеса на оценяване на риска може да се представи с три фази на протичане:

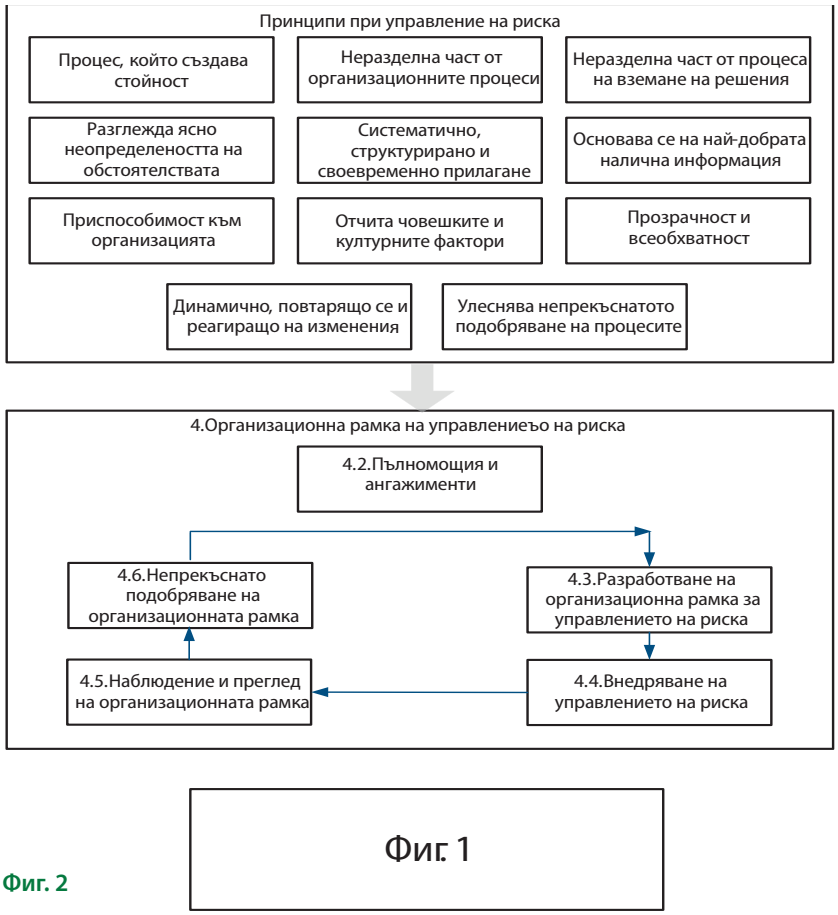
- Установяване на всички обстоятелства, свързани с риска. Това се постига чрез подходящ обмен на информаци и комуникации в рамките на организацията/дейността, която има желание да се предпази от нежелани инциденти. Установените обстоятелства могат да бъдат допълнително актуализирани, на базата на наблюдения и преглед на първоначално определените, което е като резултат от управлението на риска. Последна стъпка от тази част на процеса е определяне на критериите за риск, отчитайки установените обстоятелства и законовите изисквания за конкретна област/области;
- Оценяване на риска на база на събраната информация при установяване на обстоятелствата. В тази фаза на процеса има подпроцеси по идентификация на риска (кога, къде, как и защо). Анализът на риска е следващ подпроцес, който завършва с изчислена цифрова оценка за него. На базата на тази оценка се извършва преценка на риска съобразно зададени критерии за него. В зависимост от резултатите се вземат решения, които се подреждат в определен приоритет;
- Последната фаза на процеса е свързана с въздействие върху така определеното ниво на риск. Задължително въздействията са обект на наблюдение и преглед за оценка на ефикасността от тяхното прилагане. При тази фаза не трябва да се забравя и поддържането на обмена на информация и комуникация със заинтересованите лица, намиращи се в зоната на рисковото поле (подходяща интерпретация може да се види в нашата публикация M&E, бр. 5-6/2011).



Фиг. 1

СИСТЕМА ЗА УПРАВЛЕНИЕ НА РИСКА

Отчитайки значението на риска за всички сфери на човешката дейност, за първи път в Австралия и Нова Зеландия, се разработи и публикува стандарта за управление на риска AS/NZS 4360:2004. В него се показа една добра практика за управление на риска. Отчитайки получените резултати и значимостта на проблема международната организация по стандартизация публикува през 2009 година стандарта ISO 31000, който се базира на упоменатия по-горе национален стандарт. На фиг. 2 е показана схемата на система за управление на риска съобразно ISO 31000:2009. Анализирайки организационната рамка на управлението на риска ще се констатира, че процесът е аналогичен, както при процеса в ISO 9001 (версии 2000 и 2008). За улеснение на читателите на фиг. 3 е показан този процес.



Фиг. 2

Фиг. 1

Защитено с KASPERSKY ANTI-VIRUS www.lekarstvo.com

По конкретно приликите на ISO 31000:2009 и ISO 9001:2008 могат да се обосноват и със следните конкретни обстоятелства, присъщи и за двата стандарта. В тази насока следва да се погледнат принципите, на които почиват двата стандарта (виж БДС EN ISO 9000:2007 и началото на фиг. 2):

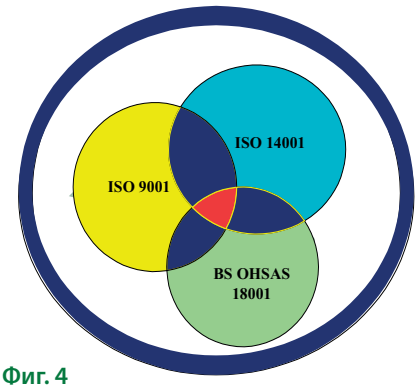
- И при двата стандарта се прилага процесния подход;
- И при двата стандарта вземането на решение се основава на факти/най-добрата информация;
- И при двата стандарта се поддържа процес на непрекъснато подобрение;
- И двата стандарта са насочени към създаване на системи за управление, които да създават стойност;
- И при двата стандарта се прилага приобщаване на персонала с отчитане на човешките и културни фактори.

Горните констатации, направени като изводи от авторския колектив в крайна сметка потвърждават обстоятелството, че всички съвременни стандарти за системи за управление (ISO 9001:2008, ISO 14001:2004, ISO/IEC 17011:2004, ISO/IEC 17020:1998, ISO/IEC 17021:2011, ISO/IEC 17024:2003, ISO/IEC 17025:2005, BS OHSAS 18001:2007, ISO 22000:2005, ISO 27001:2005, ISO 28000:2007) произтичат от стандарт ISO 9001. Новото, което следва да се отбележи за този стандарт е, че той се явява като една надстройка на цитираните стандарти за системи за управление, в т.ч. и за система за управление на качеството, съобразно ISO 9001:2008.

ИНТЕГРИРАНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА БИЗНЕСА И НА РИСКА ЗА НЕГО

За първи път през 2000 в книгата си „Ръководство за управление на риска при работа" ст.н.с. д-р инж. Илия Ценев представи идеята за съвместна работа на няколко системи за управление (ISO 9000, ISO 14000, ЗБУТ). В последващи публикации се развиват и теорията на интегрираните системи за управлени (ИСУ, фиг. 4). На практика, когато се приложат едновременно няколко системи за управление (ISO 9001:2008, ISO 14001:2004, BS OHSAS 18001:2007, ISO 22000:2005, ISO 27001:2005, ISO 28000:2007) може да се каже, че се прилага една добра практика за интегрирано управление на бизнеса. В периода 2000-2004 години представената теория за интеграция беше доказана с внедряване и сертификация на първите в България ИСУ. Повече подробности по тази тема могат да се намерят на www.praktika-ok.com.

През последните няколко години ИСУ масово се появиха в България. По мнението на авторите при голяма част от тях внедряването е формално, а сертификацията е продиктувана от икономически интереси на сертифициращите организации. Изледванията в тази насока са публикувани в M&E, бр. 1/2009 и M&E, бр. 4/2010. Текстовете могат да се вземат и от www.praktika-ok.com. Освен изказаните становища, по темата за формалното внедряване на ИСУ, чрез настоящата публикация авторите искат да внесат още доказателства. Те се базират на обстоятелството, че масово фирмите със сертифицирани ИСУ не оценяват и не управляват риска. Добре известно е, че той е от съществено значение при управление на различните структурни съставки на всеки бизнес. Направените констатации за ИСУ, а така също и за системите за управление, базиращи се на цитираните по-горе ISO&ISO/IEC - стандарти, са валидни за изследвания в България.



Фиг. 4

Във връзка с интеграция работата на системите за управление на бизнеса и система за управление на риска по ISO 31000:2009, следва да се подчертае, че този стандарт не е предназначен за целите на сертифицирането. Колекционерите на сертификати за ИСУ ще бъдат разочаровани от това обстоятелство, но такъв е характера на стандарта. Той препоръчва организациите да развиват, прилагат и непрекъснато да подобряват управлението на риска в цялостното управление на бизнес процесите. Управление на риска може да се прилага за цялата организация, или за конкретни нейни бизнес процеси, по всяко време, както и за специфични функции, проекти или дейности. При идентифициране, оценяване и управление на рисковете, организациите непрекъсното се консултират и комуникират със заинтересованите страни. За която и да е организация заинтересовани страни от управление на риска са:

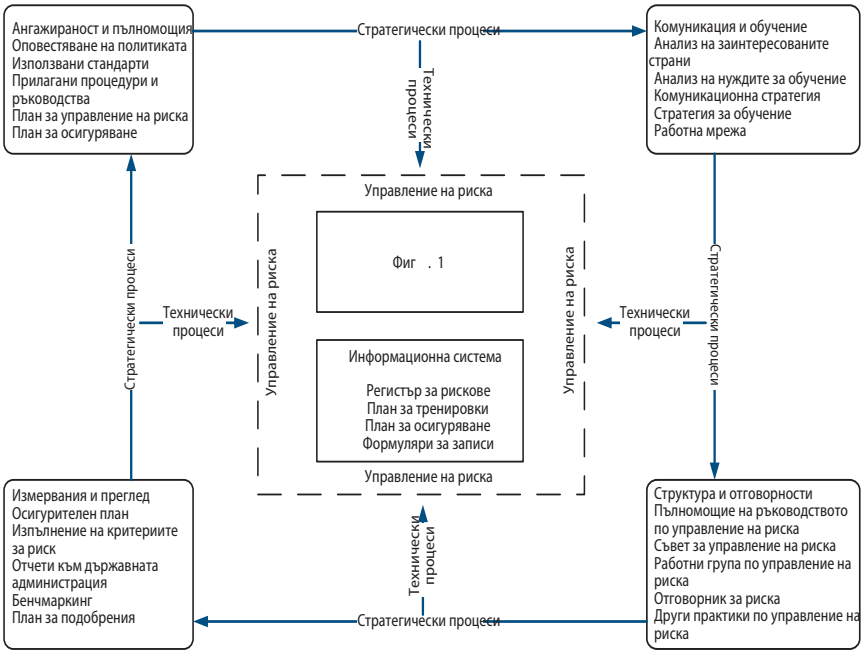
- Отговорните лица за развитието на политиката за управление на риска в рамките на тяхната организация;
- Отговорни лица за ефективното

Фиг. 3

управление на риска в рамките на организацията като цяло или в рамките на определени области, проекти или дейности;

- Персоналът, който трябва да прецени ефективността на система за управление на риска, на базата на наръчници, процедури и добри практики, които в зависимост от конкретния казус могат интегрирано да работят със системи по ISO&ISO/IEC-стандарти.

На фиг. 5 са показани протичането на стратегически и технически процеси при оценка на риска. Вижда се, че на практика те са четири: „ангажираност и пълномощия", „комуникация и обучения", „структури и отговорности". „измерване и преглед". Във всички показани по-горе системи за управление, базиращи се на ISO&ISO/IEC-стандарти съществуват идентични бизнес процеси, които са подчинени основно на качеството, околната среда, здраве и безопасност при работа, акредитация, изпитване, безопасност на храните, информационна сигурност и други. Във всички тези специфични бизнес процеси съществува определен риск, който не трябва да се пренебрегва, а напротив следва да се отчита и да се управлява, така че да се постига ефективност при неговото протичане. Ето това е новото, което се препоръчва в новия стандарт ISO 31000:2009, и което не дава основание да се извършва сертифициране по него. Видно от фиг. 5 е, че стратегическите процеси, за да протичат ефективно следва да се поддържат технически процеси, свързани с оценка на риска. Така трябва да се разбира философията на стандарта, че управление на риска се прилага за цялата организация, или за конкретни нейни бизнес процеси, по всяко време.



Фиг. 5

НАСОКИ ЗА ПРАКТИЧЕСКО ПРИЛАГАНЕ НА СЪВМЕСТНА РАБОТА НА СИСТЕМИ ЗА УПРАВЛЕНИЕ ПО ISO&ISO/IEC - СТАНДАРТИ СЪС СИСТЕМА ПО ISO 31000:2009 / ISO 31010:2009.

До сега ставаше въпрос за система за управление на риска без да се коментират методите за неговата оценка. Същите, в зависимост от конкретните бизнес процеси, подробно са разгледани в ISO 31010:2009 (БДС ISO 31010:2011). Ако риска не бъде добре интерпретиран съобразно методиката за неговата оценка (фиг. 1) то, той може сериозно да заблуди вземането на решения за последващи въздействия върху него. Възможностите в тази насока са както следва:

- Избягване на риска, като се реши да не се започне или да се спре дейност, която поражда риск;
- Приемане на съществуващ риск или дори приемане обстоятелството за неговото повишаване, за да се ползва някаква благоприятна (макар и рискова) възможност за постигане на конкретен ефект/полза (чрез определяне на механизми за наблюдение и преглед);
- Отстраняване на източника на риска, когато оценените рискове не могат да бъдат управлявани в достатъчна степен;
- Промяна на вероятността за поява на риск;
- Промяна на последствията от проява на риска;
- Споделяне на риска с друга страна или страни (използване на ресурсите на избраните партньори за управление на риска, когато това е по ефективно за организацията);
- Запазване на риска, като се определят механизми за наблюдение и преглед.
- В заключение авторите дават някои практически насоки за интегрирана работа на системи за управление по ISO&ISO/IEC - стандарти и система за управление на риска. По-долу са изброени някои конкретни рискове, свързани с протичането на бизнес процеси в конкретни системи за управление.
- За ISO 9001:2008 - реализация на продукт/услуга на конкретен пазар, погасяване на кредит към банка, приемане съответстващ продукт като несъответстващ, приемане на несъответстващ продукт като съответстващ, ритмичност в изпълнение ангажиментите на доставчиците, деформирана оценка за удовлетвореността на клиента, оценка за ефикасност на бизнес процесите, оценка за ефективност на бизнес процесите, обективна оценка за процеса на непрекъснати подобрения и други;
- За ISO 14001:2004 - деформирана оценка на аспектите на околната среда, оценка неопределеността при екологичен мониторинг на максимални/минимални прагове на параметри по околната среда, управление на отпадъци, оценка за ефикасност при прилагане на законови изисквания, оценка за ефективност на екологосъобразно управление, адекватни действия при извънредни ситуации и други;

Защитено с KASPERSKY ANTI-VIRUS www.lekarstvo.com

- За ISO/IEC 17011:2004 - акредитиране на кандидат ОС, който не отговаря на изискванията, неакредитиране на кандидат ОС, който отговаря на изискванията, ритмичност при провеждането на надзори върху работата на акредитираните лица за ОС, деформирана оценка за удовлетвореността на клиента, оценка за ефикасност на процесите при акредитация, обективна оценка на процеса на изпълнение партньорските ангажименти към MLA-споразумения и други;
- За ISO/IEC 17020:1998 - издаване на документ с положителен резултат от контрола за продукт/процес, който не отговаря на изискванията, издаване на документ с отрицателен резултат от контрола за продукт/процес, който отговаря на изискванията, оценка за ефикасност на процесите за контрола, оценка за ефективност на процесите на контрола и други;
- За ISO/IEC 17021:2011 - сертифициране на клиент със СУ, която не отговаря на изискванията, отказ от сертификат на СУ на клиент, която отговаря на изискванията, изпълнение графика за контролни одити на СУ, деформирана оценка за удовлетвореността на клиента, оценка за ефикасност на процесите при сертификация на СУ, оценка за ефективност на процесите на контрола и други;
- За ISO/IEC 17024:2003 - сертификация на персонал, който не отговаря на изискванията, отказ за издаване на сертификат за персонал, който отговаря на изискванията, деформирана оценка за удовлетвореността на клиента, оценка за ефикасност на процесите при сертификация на персонал, оценка за ефективност на процесите при оценка на персонал и други;
- За ISO/IEC 17025:2005 - оценка на реалната неопределеност при изпитване и свързаните с нея последствия, оценка на реалната неопределеност при вземане на проба и свързаните с нея последствия, оценка на реалния калибрационен интервал на ТСИ и свързаните с него последствия, деформирана оценка за удовлетвореността на клиента, издаване на протокол от изпитване, което е извън обхвата на акредитация и свързаните с това последствия, оценка за ефикасност на процесите на изпитване/пробовземане, оценка за ефективност на процесите на изпитване/пробовземане и други;
- За BS OHSAS 18001:2007 - деформирана оценка на рисковете по работните места, оценка неопределеността на максимални/минимални прагове на параметрите по здраве и безопасност, оценка за ефикасност при прилагане на законови изисквания, оценка за ефективност при управлението на здравословни и безопасни условия на труд, адекватни действия при извънредни ситуации и други;
- За ISO 22000:2005 - всичко казано за ISO 9001:2008 ориентирано към безопасността на храните;
- За ISO 27001:2005 - всичко казано за ISO 9001:2008 ориентирано към сигурността на информацията за организацията и за нейните клиенти;
- За ISO 28000:2007 - всичко казано за ISO 9001:2008 ориентирано към всички рискове по веригата на доставка.

Следващата публикация на авторския екип ще бъде насочена към конкретни примери по прилагане на БДС ISO 31010:2011.

проф. д-р инж. Илия Ценев е получил инженерно образование по електроизмервателна техника във ВМЕИ „Ленин“ (сега ТУ-София). Има защитена дисертация по проблемите на статистически методи за контрол на метрологични характеристики Хабилитацията му е по системи по качеството с използване на компютри. Притежава множество сертификати, издадени от престижни организации и институции: за специализации по метрология и компютърни технологии; за консултант по управление; за DGQ/EOQ - вътрешен одитор, TQM - мениджър; за европейски одитор по качество; за водещ одитор по околна среда (от ANSI-RAB USA); за представител на софтуер за интегрирани системи; за гост-професор по интегрирани системи за управление и други. Автор е на редица научно-изследователски публикации в областта на качество, околна среда, здраве и безопасност при работа. Управител е на “ПРАКТИКА-О.К.” ООД.

инж. Мариана Ширкова е завършила Харковски инженерно-икономически институт (Украйна). Притежава сертификати, издадени от престижни организации и институции: за OHMI EuroCert одитор; за консултант по управление (ISO 9001, ISO 14001, ISO 27001, GMP, HACCP); за гост-доцент по интегрирани системи за управление. Автор е на редица научноизследователски публикации. Има професионален опит в разработването на специализиран софтуер за управление на процедури, работни инструкции и формуляри за околна среда, коригиращи и превантивни действия и одитиране, оценка на екологичен риск, оценка на риска при работа на платформа SQL server, Service Manager. Управител е на “ПРАКТИКА-О.К.” ООД и фондация „Качество 21-ви век”.

Димитър БАНТУТОВ
експерт от „Практика-О.К.” ООД

ст.н.с. д-р Пламена ЗЛАТЕВА - БАН,
експерт към фондация „Качество 21-ви век”

инж. Недялко ИВАНОВ
„ЕКОМА“ ЕООД

д-р инж. Георги ПОПОВ
QEP - University of Central Missouri, USA