ИНТЕГРИРАНА СИСТЕМА ЗА УПРАВЛЕНИЕ НА КАЧЕСТВОТО И ИНФОРМАЦИОННАТА СИГУРНОСТ (ИСУ- КИС)

ПОДХОД ЗА ИЗГРАЖДАНЕ

А. ОСНОВНИ ПОЛОЖЕНИЯ

1. Проектирането, изграждането, внедряването, поддръжката и развитието на **ИСУ- КИС** на организацията се базира на **едновременното прилагане** на изискванията на I**SO 9001:2015**, **ISO 27001:2013** и препоръките на **ISO 27002:2013** към нейните:

- бизнес процеси;
- продукти;
- услуги;
- информационни активи;
- персонал.

2. Бизнес процесите:

- създават **продукти** и / или **услуги**, за клиентите на организацията (възможно е и за самата организация);
- се изпълняват от **персонала** (собствен и/или на подизпълнители);
- използват **информационни активи** (напр., софтуер, хардуер, информация / данни, компютърни мрежи, цялостни ИТ системи, приложения, персонал и др.), **необходими за тяхното функциониране**.

3. В **документално отношение,** ИСУ-КИС, **покрива напълно** изискванията на ISO 9001:2015 и на ISO 27001:2013, като в същото време **намалява общия брой документи** (в сравнение с броя документи, при отделно разработени системи за управление на качеството и информационната сигурност).

4. ИСУ-КИС **осигурява съответствие с изискванията** (не само за документалната част) на ISO 9001:2015 и на ISO 27001:2013, асъщо и **сертифицирането,** за степен на съответствие с тях.

5. ИСУ-КИС **намалява значително усилията и ресурси**, необходими за нейното изграждане, внедряване, поддръжка и развитие (в сравнение с необходимите усилия и ресурси, при отделно изграждани, внедрявани, поддържани и развивани системи за управление на качеството и информационната сигурност).

6. ИСУ-КИС създава **реални условия за комплексно и ефикасно управление** на **качеството и сигурността** на бизнес процесите, създаваните от тях продукти и/или услуги, използваните активи за тяхното функциониране и персонала, отговорен за тяхното изпълнение.

Б. ОБЩИ ИЗИСКВАНИЯ В ISO 9001:2015 И ISO 27001:2013

Общите изисквания в двата стандарта са в следните области:

- **Контекст на организацията** – изисква се да се определят вътрешните и външни фактори, свързани / влияещи с/на функционирането на организацията, но в две, различни перспективи – **качество** и **информационна дигурност**.

- **Заинтересувани страни и техните изисквания** – организацията трябва да определи заинтересуваните страни и техните **изисквания към качеството и информационната сигурност**. Тази дейност може да се извърши с един процес, който да създаде, като резултат, интегриан списък на заинтересованите страни и техните изисквания.

- **Отговорности и пълномощия** – организацията трябва да определи съответните отговорности и пълномощия, които са различни за Системата за управление на качеството и Системата за управление на информационната сигурност. Важното е, че тези действия могат да бъдат извършени **едновременно, по един и същи начин**.

- **Компетентност, осъзнаване, комуникации, контрол на документите и записите** (общо - документираната информация) **на системите** – изискванията, свързани с тези области са едни и същи не само за ISO 9001 и ISO 27001, но и за други стандарти (ISO). В този смисъл, тези изисквания могат да бъдат изпълнявани **едновременно, по един и същи начин**.

- **Вътрешен одит и Преглед от Ръководството** – изискванията към одитите и прегледите (като цели, резултати и др.) са различни, но начините за тяхното планиране, провеждане, документиране са едни и същи. Възможно е, одитите и/ли прегледите да се извършват едновременно, или поотделно, в съответствие с конкретните решения на Ръководството.

- **Несъответствия и корективни мерки** – процеса, свързан с разкриването на несъответствия и определяне / прилагане на корективни действия може да бъде един и същ за двата стандарта. Няма съществени причини за разделянето на този процес.

Отчитайки посочените по-горе общи области в двата стандарта, логично е да се мисли,че за тези области, системата за управление ще бъда една. Трябва да се разбере, че независимо подобните изисквания (в много случай те са еднакви) и възможността, те да бъдат постигани с един и същи процес, то получените резултати ще бъдат различни (за двата стандарта). Това се обуславя от факта, че ISO 9001 се **концентрира върху качеството на продуктите / услугите и задоволеността на клиентите**, а ISO 27001 – върху **информационната сигурност на активите**. В този смисъл, резултатите и „входовете" (входни данни / информация и др.) от / на прегледите на Ръководството ще бъдат различни. Това (различни резултати и „входове") се отнася за повечето от по-горе изброените общи области на стандартите.

В. ДОПЪЛНИТЕЛНИ ИЗИСКВАНИЯ НА ISO 27001

Разликите в изискванията на двата стандарта взаимно се допълват и обогатяват в **интерес** на подобряването на бизнеса. На практика, **информационната сигурност създава устойчивост на потенциала** на организацията, а **управлението на качеството създава този потенциал**. След определянето на общите области в стандартите, организацията трябва да отчете и разликите в тях – съдържащи се основно в изискванията от кл.6 и кл.8.

ISO 27001 добавя към ИСУ-КИС:

- **Оценка на рисковете към информационната сигурност** – Необходимо е организацията да разработи / приеме и приложи методология за разкриване, оценка и анализ на рисковете към информационната сигурност. **ВАЖНО** – този процес **НЕ ТРЯБВА** да бъде смесван с процеса за **оценка на рисковете и възможностите** в ISO 9001. На практика, използваната методология за анализ и оценка нарисковете към информационната сигурност, може да бъде **опростена** и **прилагана**, и за съответните

изисквания на ISO 9001 (рискове и възможности, отчитайки контекста на организацията). Разбира се, напълно примливо и приложимо е (дори е препоръчително), да се използва **друга методология** (в сравнение с тази по информационната сигурноста) за рисковете и възможностите.

- **Противодействие на разкритите рискове към информационната сигурност** – Този процес **не съществува**, като изискване в ISO 9001 и затова трябва да бъде изпълнен самостоятелно. Процеса изисква най-малко, внедряването на контролни / защитни механизми, избрани от описаните в **Приложение А** на **ISO 27001**.

Г. ПОЛЗИ ОТ ИЗГРАЖДАНЕТО НА ИСУ-КИС

Чрез интегрирането на двете системи (за управлениена качеството – СУК и управлениена информационната сигурност - СУИС) се получават реални възможности, позволяващи **комбиниране на ресурсите, а от там и спестяване на време и пари, а също и цялостно подобряване на системата за управление**. В допълнение чрез изграждането и внедряването на ИСУ-КИС, организацията може ясно да покаже / докаже качеството и сигурността на своите бизнес процеси, а също, по този начин да придобие високи конкерентноспособност, репутация, намаляване на рисковете и задоволяване на изискванията на клиентите.

В **ПРИЛОЖЕНИЕ 1** (ANNEX1_MATRIX_ISO 9001_ISO 27001) към този документ, в интерес на изграждането на ИСУ- КИС са показани:

- клаузите на двата стандарта;
- връзките между клаузите на двата стандарта;
- документалната част на двата стандарта (задължителни и препоръчителни за разработване документи);
- документалната част на ИСУ – КИС (задължителни и препоръчителни за разработване документи), като резултат от интегрирания подход за изграждане на системата.