

**Информация за политиката на Ем Джи Глобал за прехода към
ISO 27001:2022, съгласно изискванията на ИА БСА, публикувани на
19.12.2022г**

1. Обща информация

На страницата на Международната организация по стандартизация (ISO) през октомври е публикуван стандарт ISO/IEC 27001:2022 „Сигурност на информацията, киберсигурност и защита на поверителността. Системи за управление на сигурността на информацията. Изисквания“. Той отменя и заменя ISO/IEC 27001:2013.

В съответствие с изискванията на прехода към новата версия на стандарта ISO/IEC 27001:2022, публикувани в документа IAF MD 26:2022 от 09.08.2022 г., преходният период завършва на 31.10.2025г.

С настоящата информация Ем Джи Глобал представя подход в съответствие с промените, който ще използва като орган за сертификация извършващ сертификация на Системи за управление на сигурността на информацията (СУСИ), да демонстрира съответствието си с изискванията на промените в ISO 27001:2022, в рамките на определения от Международния Акредитационен Форум срок.

2. Подход на Ем Джи Глобал за въвеждане на изискванията на ISO 27001:2022 и срокове

ISO 27002:2022 адресира промените както в средата на кибер заплахите в която организациите работят в момента, така и в техническата зрялост на тактиките, техниките и процедурите, които могат да се прилагат като контрол на сигурността. Скорошното навлизане на облачни технологии, хибридни работни практики (ускорени от пандемията Covid-19) и отговорностите за сигурността и последиците, които това създава, са разгледани в това последно издание на ISO 27002. Указателният документ вече позволява на организациите да използват динамична рамка, която може да се напасва както за самата организация, така и за заплахите, отправени към нея от злонамерени участници.

Новите контроли, които документът с указания въвежда заедно с неговото реструктуриране, ще повлияят на няколко области от СУСИ на организацията, включително Декларацията за приложимост и плановете за третиране на риска.

Съгласно изискванията на ИА БСА, (публикувани на 19/12/2022г.) до 31.10.2023г. е извършена оценка от страна на ИА БСА по време на планов надзор.

След получаване на акредитация по новата версия на стандарта ISO/IEC 27001:2022, всички сертификационни одити на системи за управление на сигурността на информацията за нови клиенти ще бъдат извършвани спрямо изискванията на ISO 27001:2022.

За настоящи клиенти със сертифицирани системи за управление на сигурността на информацията:

- Преминването от ISO 27001:2013 към ISO 27001:2022 може да се осъществи по време на едно посещение. За да се оценят извършените промени и ефективността на внедряването, към продължителността на одита се добавя допълнително минимум един одит ден.
- Ако сертификатът по ISO 27001:2013 на клиент изтича преди да са успели напълно да извършат миграция към ISO 27001:2022, може да се извърши ресертификация спрямо ISO 27001:2013 (при условие, че крайния срок позволява преход при следващо посещение). След 30.04.2024 всички Сертификационни и Ресертификационни одити ще се извършват само спрямо ISO 27001:2022.
- Сертификат за ISO 27001:2022 ще бъде издаден, когато може да бъде задоволително доказано, че клиентът е изпълнил изцяло изискванията на новата версия на стандарта. Както е в сегашната практика, всички значителни несъответствия трябва да бъдат официално закрити и коригиращите действия за незначителните несъответствия трябва да бъдат получени и приети от Ем Джи Глобал ООД, преди издаването на сертификат.
- Преди да бъде извършен одитът за преход, от клиентите се изисква да попълнят документа на Ем Джи Глобал ООД ISO 27001:2022 Гап Анализ. Клиентите също се насърчават да извършат вътрешен одит и преглед от ръководството спрямо новия стандарт, тъй като това ще послужи както за да се гарантира, че всички изисквания са разгледани в системата за управление на клиента, така и за да се осигури лесно позоваване на тези изисквания по време на миграционния одит. Като минимум, клиентът трябва да е извършил официален гап анализ като е използвал споменатия по-горе документ и е прегледал резултатите с висшето ръководство на преглед от ръководството или еквивалентен механизъм.

Миграциите ще се извършват по време на годишен надзорен или ресертификационен одит. Към продължителността на одита ще бъде добавено допълнително време за да се даде възможност да се извърши пълна и ефективна оценка на миграцията спрямо новите изисквания на стандарта. Допълнителното време ще бъде минимум един одит ден. Според спецификите на организацията може да е необходимо допълнително време. Това ще бъде определено от Ем Джи Глобал ООД.

По изключение - Миграциите могат да се провеждат като специално посещение по искане на клиента. При тези обстоятелства продължителността трябва да бъде минимум един одит-ден.

Тъй като изискванията за определяне на времето за одит са променени, договорите между Ем Джи Глобал и клиентите ще бъдат преразгледани за да следват новите изисквания, при предстоящ одит за преход.