Тема 7. Сертифікація ІТ послуг. Схеми сертифікації

Сертифікація – це як гарантійний талон для замовника, який підтверджує відповідність вашого бізнесу міжнародним стандартам, а ще – готовність до будь-яких форс мажорів.

Розробкою й публікацією світових стандартів опікується Міжнародна організація зі стандартизації (ISO). Підготовка таких норм проводиться для різних сфер: медицини, кібербезпеки, управління довкіллям, енергоспоживання тощо.

Для кожної сфери, звичайно, розроблені свої стандарти. Всі вони унікальні та кожен покриває свою окрему частину процесів. Для ІТ-сфери, банків, дата-центрів найпоширенішими є стандарти ISO/IEC 27001 (СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ), ISO/IEC 27701 (СИСТЕМА УПРАВЛІННЯ ПЕРСОНАЛЬНИМИ ДАНИМИ).

Основні переваги ISO/IEC 27001

ISO/IEC 27001 – це підтвердження того, що система управління інформаційної безпеки в компанії знаходиться в в контрольованих умовах. Як мінімум розроблені базові заходи (якщо в ISO/IEC 27001 це заходи управління інформаційною безпекою, то в ISO/IEC 27701 це вже управління персональними даними) реагування на кризові явища, а отже бізнес в надійних руках.

Сертифікат визнається на світовому рівні, тому у вас є гарна можливість виходу на іноземні ринки та активного залучення зарубіжних партнерів. Наприклад, в країнах ЄС і США наявність таких сертифікатів є нормою, а їх відсутність – відповідно, фактор ризику.

Підготовка до сертифікації

Термін підготовки залежить, у більшій мірі, від рівня злагодженості процесів у компанії, тому може тривати від трьох місяців до двох років. Даний етап включає:

- навчання персоналу;
- проведення діагностичного аудиту (GAP аналізу);
- розробку політики та процедур, необхідних в стандарті (наприклад, політики та цілі інформаційної безпеки, реєстр активів, оцінка інформаційних ризиків компанії, політика управління персоналом, політика забезпечення фізичної безпеки, операційні процедури для управління IT та багато інших);
- інформаційні активи компанії займають особливе місце при розробці та аудиті: наскільки вони визначені та захищені.

Проведення сертифікації. Такий процес може зайняти близько 1-2 місяців і включає в себе кілька стадій.

Наприклад, для ISO/IEC 27001 на першій стадії відбувається аналіз документації і внутрішній аудит. Якщо перша стадія пройшла успішно, то планується друга стадія.

На другій стадії аудитор проводить інтервью з персоналом.

Вартість та терміни виконання обох етапів може залежати від сфери діяльності, кількості персоналу, кількості фізичних локацій компанії, тощо.

Сертифікат видається на 3 роки та кожен рік проходить наглядовий аудит. Компанії треба довести, що вона продовжує відповідати вимогам стандарту.

Звичайно, якщо у вас є потреба в отриманні такого сертифікату, ви сміливо можете звернутися до сертифікаційних органів в Україні. Найкраще при цьому буде передати цей процес компанії, яка має великий досвід, базу партнерів та репутацію на ринку.