Proces certyfikacji systemu zarządzania bezpieczeństwem informacji wg ISO 27001

Wstęp

System zarządzania bezpieczeństwem informacji (SZBI) jest częścią ogólnego systemu zarządzania organizacją, która obejmuje: strukturę organizacyjną, planowanie, odpowiedzialności, zasady postępowania, procedury, procesy i zasoby potrzebne do opracowania, wdrażania, realizowania, przeglądu i utrzymywania polityki bezpieczeństwa informacji.

Aby zapewnić ciągłe doskonalenie systemu oraz potwierdzić jego zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2017-06, SZBI poddawany jest audytom (auditom*).

Audyt systemu bezpieczeństwa informacji to systematyczne i niezależne badanie, mające na celu określenie:

- czy działania podejmowane w ramach SZBI oraz osiągnięte rezultaty odpowiadają planowanym ustaleniom

- czy ww. ustalenia zostały skutecznie wdrożone

- czy ww. ustalenia są odpowiednie do realizacji polityki bezpieczeństwa informacji, a także do osiągnięcia celów organizacji w tym zakresie.

*Słowa „audit" i „audyt" uznaje się za równoważne.

Proces certyfikacji

Certyfikacja SZBI prowadzona w DEKRA Certification Sp. z o.o. (dalej: DEKRA) jest w równym stopniu dostępna dla wszystkich organizacji, niezależnie od formy prawnej, reprezentowanej branży, wielkości zatrudnienia, osiąganych wyników itp.

Proces certyfikacji rozpoczyna zapytanie od zainteresowanej uzyskaniem certyfikatu organizacji, bądź ogłoszenie o przetargu publicznym, a następnie złożenie przez organizację podpisanego przez osobę uprawnioną wniosku o przeprowadzenie certyfikacji (formularz przesyła do zainteresowanej organizacji pracownik DEKRA).

Kompletny wniosek, wraz z wymaganymi załącznikami, poddawany jest analizie przez koordynatora DEKRA, który ocenia możliwość realizacji procesu certyfikacji SZBI. Po uzyskaniu pozytywnej oceny podpisywana jest umowa na certyfikację.

Audyt certyfikacyjny SZBI realizowany jest w 2 fazach. Warunkiem przystąpienia DEKRA do audytu jest zapewnienie przez klienta właściwych warunków dostępu do informacji poufnych lub wrażliwych.

1 Faza audytu (1 etap)

Celem pierwszej fazy audytu jest ocena dokumentacji SZBI, otrzymanie informacji o SZBI w kontekście organizacji klienta, szacowania i postępowania z ryzykiem (w tym określonych zabezpieczeń), polityki i celów bezpieczeństwa informacji oraz określenie gotowości do drugiego etapu audytu, zebranie niezbędnych informacji dotyczących zakresu systemu zarządzania, uzgodnienie z klientem szczegółów drugiego etapu.

Zespół audytorów dokonuje przeglądu dokumentacji SZBI, w tym Deklaracji Stosowania. U klienta będzie weryfikowany fakt posiadania co najmniej jednej Deklaracji Stosowania w zakresie certyfikacji. Przegląd obejmuje ocenę zgodności systemu z kryteriami audytu (np. ISO 27001, wymagania prawne). Klient zostanie poinformowany o dodatkowych rodzajach informacji i zapisach, jakie mogą być wymagane do szczegółowej oceny podczas 2 fazy audytu.

2 Faza audytu (2 etap)

Celem drugiej fazy audytu jest ocena spełnienia wymagań SZBI w organizacji klienta, ocena usunięcia niezgodności z pierwszej fazy audytu (o ile nie zostały one jeszcze zamknięte) oraz

potwierdzenie, że organizacja klienta przestrzega własnej polityki, swoich celów oraz procedur bezpieczeństwa informacji.

Audytorzy oceniają, czy szacowanie ryzyka i postepowanie z ryzykiem w bezpieczeństwie informacji u klienta właściwie odzwierciedla zakres działalności klienta i czy rozciągają się one po granice jego działalności. Audyt ma na celu ocenić, czy na podstawie szacowania ryzyka klient wdrożył dające się zastosować zabezpieczenia i osiągnął ustalone cele bezpieczeństwa informacji.

DEKRA ustala ponadto, czy procedury klienta dotyczące identyfikacji, sprawdzenia i oceny ryzyka zawiązanego z bezpieczeństwem informacji oraz wyniki ich wdrożenia są zgodne z polityką organizacji klienta, celami i zadaniami oraz ustali czy procedury stasowane do szacowania ryzyka są godne zaufania i prawidłowo wdrożone.

Audyt nadzorujący

Podczas 3-letniego okresu trwania ważności certyfikatu odbywają się coroczne audyty nadzorujące (audyt nadzoru).

Pierwszy audyt nadzoru musi zostać przeprowadzony w okresie nieprzekraczającym 12 miesięcy od dnia uzyskania certyfikatu.

Audyt nadzorujący ma na celu:

- weryfikację wdrożenia SZBI

- wpływu jaki na SZBI maja zmiany zainicjowane zmieniającymi się działaniami u klienta

- potwierdzenie ciągłej zgodności z wymaganiami certyfikacji.

Program nadzoru jest dostosowywany do zagadnień bezpieczeństwa informacji związanych z rodzajami ryzyka oraz skutkami dla klienta. Weryfikacji i udokumentowaniu podlegają działania korygujące w stosunku do niezgodności z poprzedniego audytu.

Audyt recertyfikujący (wznawiający)

Aby zapewnić przedłużenie ważności certyfikatu na kolejne 3 lata konieczne jest przeprowadzenie audytu wznawiającego.

Audyt recertyfikujący powinien być przeprowadzony przed upływem ważności certyfikatu.

Audyt recertyfikujący ma na celu weryfikację skuteczności systemu zarządzania w organizacji klienta. Wymagania audytu wznawiającego są podobne do wymagań audytu certyfikacyjnego.