

Czym jest certyfikacja ISO 27001?

ISO/IEC 27001 jest normą standaryzującą system zarządzania bezpieczeństwem informacji (ISMS), opublikowaną w październiku 2005 przez Międzynarodową Organizację Normalizacyjną oraz Międzynarodową Komisję Elektrotechniczną. ISO27001 zastępuje ISO17799 i BS 7799, stając się jedynym certyfikowanym standardem zarządzania bezpieczeństwem. Certyfikacja ta jest powszechnie uznawanym dowodem jakości programu bezpieczeństwa danej organizacji.

Które z usług Websense posiadają certyfikat ISO 27001?

Usługi Websense Hosted Email Security (ochrona poczty elektronicznej) oraz Websense Hosted Web Security (bezpieczeństwo sieci Web), po przejściu drobiazgowej i rygorystycznej weryfikacji, otrzymały certyfikat ISO 27001 we wrześniu 2006. Certyfikat dla usług Websense został przedłużony przez SGS UK Ltd. we wrześniu 2009, a co sześć miesięcy przeprowadzane są zewnętrzne audyty służące kontroli jakości.

Jakie korzyści wynikają z posiadania certyfikatu ISO 27001?

Pomaga spełnić wymagania legislacyjne obowiązujące w Stanach Zjednoczonych:

- Sarbanes-Oxley Act z 2002 roku, Sekcja 404,
- wymagania SAS 70,
- wymagania HIPAA (reguła bezpieczeństwa),
- Gramm Leach Bliley Act z 1999 roku,
- kalifornijskie prawa dotyczące prywatności, z uwzględnieniem SB 1386.

W sposób pośredni spełnia wymagania legislacyjne i zapewnia zgodność z regulacjami prawnymi, takimi jak:

- Legislacja regulująca kwestie prywatności, w tym regionalne uchwały dotyczące ochrony danych.
- Międzynarodowe wymagania legislacyjne.

Usprawnia program zarządzania dostawcami:

- Organizacje preferują dostawców będących w stanie udowodnić fakt spełnienia przez nich najwyższych standardów.
- Certyfikacja może być wymagana przez klientów specyficznych rynków, takich jak sektor finansowy, centra danych, czy też dostawcy usług online.

Zapewnia wskaźnik i niezależny dowód na to, iż najlepsze praktyki branżowe są uwzględniane jako część korporacyjnego programu zarządzania:

- Korporacje muszą nieprzerwanie zabiegać o egzekwowanie najlepszych praktyk, często bowiem zachodzi potrzeba wykazania udziałowcom, w tym sponsorom, wspólnikom i finansistom, że w należyty sposób troszczą się one o bezpieczeństwo informacji.
- ISO 27001 oferuje konkurencyjne różnicowanie w porównaniu z innymi, mniej rygorystycznymi certyfikatami.

Czym certyfikacja ISO 27001 różni się od certyfikacji SAS 70?

SAS 70 określa standardy stosowane przez audytora usługi w celu oceny wewnętrznych mechanizmów kontrolnych organizacji świadczącej usługi oraz stworzenia raportu audytora usługi.

- Nie jest to norma bezpieczeństwa, a jedynie metoda, dostarczająca ujednoliconego formatu raportowania.
- W żaden sposób nie gwarantuje ona egzekwowania korporacyjnych norm bezpieczeństwa informacji.
- SAS 70 znajduje zastosowanie jedynie dla operacji objętych legislacją Stanów Zjednoczonych.

Certyfikacja ISO 27001 gwarantuje kierownictwu, partnerom biznesowym, klientom i audytorom poważne i rzetelne podejście organizacji do kwestii zarządzania bezpieczeństwem informacji.

- Zapewnia większe bezpieczeństwo informacji, ponieważ standard został zaprojektowany specjalnie, aby zaadresować aktualne najlepsze praktyki w dziedzinie bezpieczeństwa informacji.
- Jest ona nieporównywalnie bardziej obiektywna niż alternatywne standardy bezpieczeństwa.
- Zgodność z normą ISO 27001 jest weryfikowana w kontekście spełniania zestawu obowiązkowych klauzul, opublikowanych przez Międzynarodową Organizację Normalizacyjną.
- Zgodność z normą ISO 27001 gwarantuje, iż korporacja spełnia odpowiednie procedury dostarczania usługi, takie jak kontrola zmian, autoryzacja i inne procedury operacyjne, a także w stosowny sposób zarządza zasobami i podziałem obowiązków.
- ISO 27001 jest powszechnie uznawaną przez branżowych ekspertów normą bezpieczeństwa informacji, w przeciwieństwie do SAS 70.

