

Informacja dla Klienta – Przebieg auditów - ISO 28000:2007

Wprowadzenie

Niniejsza „Informacja dla Klienta” zawiera wyjaśnienia dotyczące głównych etapów auditowania i certyfikacji Systemu Zarządzania Bezpieczeństwem Łańcucha Dostaw (ISO 28000:2007). Proces certyfikacji wymaga zwykle dwóch wizyt w Państwa firmie zanim zostanie wydana rekomendacja. Wizyty te nazywamy:

- Etapem 1 [przeгляд systemu, ocena identyfikacji zagrożeń i oceny ryzyka bezpieczeństwa i planowanie Etapu 2]
- Etapem 2 [ocena funkcjonowania i skuteczności systemu].

Po przyznaniu certyfikatu będziemy prowadzić audyty kontrolne, które pozwolą Państwu go utrzymać.

W czasie każdej wizyty nasi auditorzy będą służyć Państwu pomocą oraz zwrócą uwagę na praktyczne aspekty omawianych zagadnień. W naszym przekonaniu stanowi to wartość dodaną świadczoną przez nas usługi. W skład zespołu auditorów wchodzi auditor wiodący, któremu może towarzyszyć jeden lub większa liczba auditorów i/lub ekspertów, w zależności od wielkości i złożoności Państwa organizacji.

Przed przybyciem, uzgodnimy z Państwem termin wizyty, godzinę jej rozpoczęcia i zakończenia, skład zespołu auditorów, długość naszego pobytu oraz obszary firmy, które odwiedzimy. Językiem auditów i raportów będzie oficjalny język przyjęty w Państwa kraju, chyba że dojdzie do innych ustaleń.

Aby umożliwić nam jak najlepsze spełnienie Państwa potrzeb podczas realizacji usługi, prosimy o wypełnienie dostarczonego przez nas formularza informacyjnego jeszcze przed naszą wizytą. Prosimy o dołączenie do formularza mapy, planu i/lub fotografii z lotu ptaka lokalizacji firmy będącej przedmiotem certyfikacji.

Analiza braków

Chociaż nie jest to wymogiem certyfikacji, LRQA zapewnia możliwość przeprowadzenia analizy braków. Analiza ta może dotyczyć na przykład:

- przeprowadzonego przez Państwa szacowania ryzyka bezpieczeństwa oraz jak zidentyfikowane ryzyko zostało odzwierciedlone w Waszych celach zarządzania
- przeglądu systemów
- przeglądu dokumentacji
- planowania i przygotowania wdrożenia lub
- innych uzgodnionych elementów.

Analiza braków jest podobna do etapu 1 oceny systemu zarządzania względem wymagań normy ISO 28000.

Etap 1 – Przegląd systemu i planowanie

Cel wizyty

Nasza wizyta ma na celu:

- ustalenie, czy wymagane przez standard ISO28000 polityki, procesy, procedury i istotna dokumentacja zostały wdrożone i są stosowane w taki sposób, że możliwe będzie przeprowadzenie etapu 2 certyfikacji
- zebranie informacji na temat sposobu organizacji, procesów i działalności Państwa przedsiębiorstwa, które umożliwią zaplanowanie etapu 2
- potwierdzenie, że szczegóły i charakter prowadzonej działalności leży w zakresie ISO 28000, z uwzględnieniem ograniczeń fizycznych i logicznych.
- potwierdzenie oczekiwań zespołu auditorów i terminu etapu 2
- udzielenie odpowiedzi na wszelkie pytania, dotyczące naszej usługi.

W ramach etapu 1 przeprowadzona zostanie pełna ocena następujących zagadnień:

- Szacowanie ryzyka bezpieczeństwa
 - Identyfikacja zasobów
 - Rozpoznanie źródeł zagrożenia
 - Analiza konsekwencji
 - Przegląd i analiza podatności
 - Ewaluacja prawdopodobieństw
- Wizja lokalna na terenie firmy, potwierdzenie zasobów i podatności
- Metodologia SRA (Safety risk assessment)
- Wartościowanie i ocena ryzyka
- Ograniczanie i planowanie ryzyka
 - Wyniki SRA jako dane wyjściowe dla „Celów i zadań” systemu zarządzania
 - Planowanie i wdrażanie zabezpieczeń [sterowanie operacyjne (procedury, personel i technologia)] w ramach zarządzania celami i zadaniami.

Ponadto:

- Ustalimy, czy są Państwo gotowi do etapu 2 certyfikacji systemu zarządzania, uwzględniając przy tym audyty wewnętrzne i przegląd zarządzania
- Ocenimy dokumentację pod kątem jej zgodności z ISO 28000
- Odnotujemy swoje spostrzeżenia i wnioski.

Podczas tej wizyty wskażemy wszelkie słabości lub braki Państwa systemu, które należy usunąć przed drugim etapem certyfikacji, podczas którego skupiamy się na sposobie jego wdrożenia.

Przebieg wizyty

Wizyta (której długość zależy od wielkości i złożoności państwa organizacji) rozpoczyna się spotkaniem otwierającym. Auditor wiodący przedstawi na nim swój zespół, wyjaśni kierownictwu sposób prowadzenia auditu, a Państwo będą mogli przedstawić swoją firmę. Auditor uzgodni też z Państwem plan wizyty.

Następnie auditor(rzy):

- zweryfikuje strukturę i dokumentację Państwa systemu w kontekście wymogów standardu ISO28000 i proponowanego zakresu oceny
- przeprowadzi wizję lokalną w celu weryfikacji: planów zakładu (żeby stwierdzić m.in. obecność budynków, wyposażenia i rozwiązań bezpieczeństwa, sąsiedztwo), potwierdzenia potencjalnych zagrożeń dla bezpieczeństwa łańcucha dostaw, identyfikacji stosowanych środków kontroli i ich wykorzystania, a także w celu zapoznania się z zakładem na potrzeby etapu 2 certyfikacji
- sporządzi szczegółowy raport, w którym ujmie zarówno swoje pozytywne spostrzeżenia, jak i wszelkie zagadnienia wymagające podjęcia przez Państwa działań przed rozpoczęciem etapu 2. W raporcie zostanie również, w celach informacyjnych, podana potencjalna gradacja tych zagadnień w przypadku gdyby nie udało się ich wyeliminować do końca etapu 2
- sporządzi szczegółowy plan etapu 2 certyfikacji.



W tym celu auditor(rzy) zwykle dokona oceny:

- **polityki bezpieczeństwa łańcucha dostaw**
- **zakresu Systemu Zarządzania Bezpieczeństwem ISO28000**
- **Rejestru Zasobów Bezpieczeństwa**
- **szacowania ryzyka i zagrożeń oraz dobozem środków kontroli**
- **podziału głównych ról i obowiązków**
- **zagrożeń dla bezpieczeństwa łańcucha dostaw** – ocena zidentyfikowanych zagrożeń dla bezpieczeństwa łańcucha dostaw i związanych z nimi ryzyk oraz ustalenie ich znaczenia dla tej części łańcucha dostaw, który Państwa organizacja powinna kontrolować lub na który powinna mieć wpływ
- **przestrzegania wymogów prawa** – ocena dostępności odpowiednich przepisów prawa i innych uregulowań (firmowych, rządowych i międzyrządowych, zarówno obowiązujących, jak i opcjonalnych), umów z instytucjami regulacyjnymi oraz wszelkich innych wymogów firmowych lub korporacyjnych i ich związku z Państwem z systemami zarządzania bezpieczeństwem
- **procesu ciągłego doskonalenia** – ocena celów i ich zgodności z przyjętą polityką; sprawdzenie, czy cele zostały ustalone i czy wspierają proces ciągłego doskonalenia, czy opracowano stosowne plany umożliwiające realizację tych celów oraz czy zajęto się zagadnieniem pomiaru wyników i ich raportowania.
- **rozwiązań operacyjnych** – potwierdzenie, że ustanowiono procedury w celu ograniczenia i nadzoru nad znaczącymi zagrożeniami dla łańcuch dostaw.
- **monitorowania i pomiarów** – potwierdzenie, że istnieją właściwe mechanizmy monitorowania i pomiarów osiągnięć bezpieczeństwa łańcucha dostaw zarówno w Państwa organizacji, jak i u podwykonawców, którzy mogą mieć wpływ na Państwa łańcuch dostaw, będących pod Waszą kontrolą lub na których macie wpływ. Ponadto, weryfikacja skuteczności systemu zarządzania, w tym postęp w realizacji założeń i celów, oraz weryfikacja utrzymywania i skuteczności środków kontroli ryzyka.

Oraz zweryfikuje procedury funkcjonujące w zakresie następujących wymogów standardu:

- **nadzór nad dokumentami**
- **nadzór nad zapisami**
- **działania korygujące**
- **działania zapobiegawcze**
- **audyty wewnętrzne i proces przeglądu zarządzania**
- procedury operacyjne dotyczące bezpieczeństwa łańcucha dostaw.

W czasie auditu, zespół auditorów, korzystając z odpowiednich metod pobierania próby, zgromadzi i zweryfikuje informacje odpowiadające celom, zakresowi i kryteriom auditu, w tym informacje dotyczące **relacji** pomiędzy funkcjami, czynnościami i procesami. **Aby stanowić dowody z auditu, informacje te muszą być weryfikowalne i odnotowane** zgodnie z wymogami ISO 19011:2002, 6.5.4.

Wizyta kończy się spotkaniem zamykającym, na którym przedstawiany jest raport z etapu 1 i dokonuje się uzgodnień dotyczących kolejnego etapu certyfikacji, w tym wszelkich zagadnień związanych z zapewnieniem dostępu do auditowanych obszarów, BHP w trakcie auditu, bezpieczeństwem i sprawami administracyjnymi.

Wszelkie sprawy wymagające uwagi i **rozważenia** zostaną **odnotowane i sklasyfikowane** w Rejestrze **spostrzeżeń** z auditu, który stanowi część raportu z pierwszego etapu certyfikacji LRQA.

Dokumentacja **przejrzana** podczas pierwszego etapu certyfikacji będzie dla nas punktem odniesienia podczas kolejnych wizyt. Powinni Państwo jednak nadal aktualizować swoje dokumenty systemowe w

ramach wewnętrznego procesu doskonalenia. Podczas każdej wizyty będziemy musieli ustalić różnice pomiędzy wersją aktualną, a wersją poprzednią.

W przypadku **stwierdzenia większych niezgodności w odniesieniu do istotnych procesów** zarządzania bezpieczeństwem, takich jak **identyfikacja zagrożeń** i ocena ryzyka, planowanie **postępowania z zagrożeniami**, lub udokumentowanych procedur **sterowania operacyjnego**, auditor wiodący zespołu auditorów LRQA może zalecić przełożenie drugiego etapu certyfikacji do czasu, aż przeprowadzone zostaną zadowalające działania korygujące i ustalić z Państwem szczegóły wizyty **dodatkowej**.

W części poświęconej raportowaniu poniżej, znajdą Państwo informację o tym, w jaki sposób **klasyfikujemy** swoje spostrzeżenia.

Etap 2 – Ocena funkcjonowania

Cel wizyty

Podczas tej wizyty auditor skoncentruje się na tym, jak Państwa system zarządzania funkcjonuje w praktyce i w jaki sposób dobrano sterowanie operacyjne, w zakresie bezpieczeństwa łańcucha dostaw, w celu zarządzania ryzykiem.

Celem etapu 2 jest sprawdzenie, czy:

- Państwa polityka, cele, programy i procedury są skutecznie realizowane
- zidentyfikowaliście Państwo zakres łańcucha dostaw kontrolowany przez Państwa organizację lub znajdujący się pod jej wpływem
- zarządzacie Państwo istotnymi procesami bezpieczeństwa, w ramach systemu zarządzania
- sterowanie operacyjne jest właściwe dla realizacji celów związanych z ograniczaniem ryzyka
- system zarządzania spełnia wszystkie wymagania standardu ISO28000 oraz został przez Państwa wdrożony i oceniony pod kątem skuteczności.

Przebieg wizyty

Audit prowadzony jest zgodnie z planem przygotowanym podczas etapu 1 wizyty. Członkowie zespołu auditorów odwiedzą poszczególne obszary firmy z przewodnikami, którzy będą świadkami spostrzeżeń zespołu i pomogą w ich ocenie. W ramach etapu 2 najczęściej odbywa się również spotkanie z przedstawicielem wyższej kadry zarządzającej, odpowiedzialnym za całość systemu zarządzania.

W raporcie naszego zespołu oceniającego zawarte zostaną spostrzeżenia w odniesieniu do co najmniej następujących zagadnień:

- działania przeprowadzone w stosunku do spostrzeżeń z etapu 1 wizyty
- działalności, które zostały zidentyfikowane w uzgodnionym zakresie auditu
- jak skuteczny jest systemu zarządzania dla realizacji zobowiązań zawartych w polityce bezpieczeństwa Państwa firmy, w tym dla procesu ciągłego doskonalenia i zgodności z wymaganiami prawa i innymi wymaganiami do których spełniania się Państwo zobowiązali.
- praktyczne stosowanie rozwiązań przyjętych w celu ograniczania ryzyka i kontroli istotnych zagrożeń dla bezpieczeństwa w łańcuchu dostaw,
- postęp w osiąganiu celów i zadań poprzez realizację programów zarządzania
- praktyczne stosowanie dokumentacji wymaganej w systemie zarządzania oraz prowadzenie odpowiednich zapisów
- praktyczne stosowanie rozwiązań w zakresie monitorowania i pomiarów, w celu oceny skuteczności systemu zarządzania oraz realizacji celów
- w jakim stopniu wyższa kadra zarządzającej jest zaangażowana w wykorzystaniu systemu zarządzania oraz
- jak skutecznie realizowane są procesy auditów wewnętrznych, działań korygujących i zapobiegawczych oraz przeglądu zarządzania.

Zespół auditorów będzie się z Państwem spotykał codziennie, w celu omówienia swoich spostrzeżeń. Należy wówczas zapewnić obecność odpowiednich pracowników, którzy będą mogli je zaakceptować. W części poświęconej raportowaniu poniżej, znajdą Państwo informacje o tym, w jaki sposób klasyfikujemy swoje spostrzeżenia. Ostateczna klasyfikacja tych spostrzeżeń zostanie ustalona na zakończenie wizyty.

Wizyta kończy się spotkaniem zamykającym, na którym podsumowujemy swoje spostrzeżenia i uzgadniamy następny etap procesu certyfikacji. W miarę możliwości, jeszcze przed opuszczeniem Państwa firmy, auditor przekaze przedstawicielowi kierownictwa kompletny raport z auditu. Jeżeli podczas wizyty nie stwierdzimy żadnych Większych niezgodności, a dla Mniejszych niezgodności będą Państwo w stanie zaproponować auditorowi działania korygujące, auditor rekomenduje przyznanie certyfikatu ISO28000 (choć zależy to jeszcze od wyników niezależnego, technicznego przeglądu, który przeprowadzimy w naszym biurze). Jeżeli jednak stwierdzone zostaną jakiekolwiek Większe niezgodności, to przyznanie certyfikatu zostanie odłożone do czasu oceny przeprowadzonych przez Państwa działań korygujących. Auditor wiodący zespołu auditorów uzgodni z Państwem termin dodatkowego auditu weryfikacyjnego. Jeżeli stwierdzone zostaną jakiekolwiek Mniejsze niezgodności, to będą Państwo musieli przedstawić swój plan działań korygujących, zanim będziemy mogli wydać pozytywną rekomendację.

Audyty kontrolne

Cel wizyty

Kiedy już Państwa system zarządzania uzyska stosowny certyfikat, rozpoczniemy realizację programu auditów kontrolnych (które typowo odbywają się co sześć miesięcy). Celem prowadzenia auditów kontrolnych jest potwierdzenie, że certyfikowany system zarządzania:

- jest utrzymywany
- jest stosowany
- przyczynia się do ciągłego doskonalenia.

Sprawdzamy również, jaki wpływ mają zmiany wprowadzane do systemu. Zmiany te mogły powstać na skutek zmiany Państwa działalności, produktów lub usług.

Następnie ocenimy, czy nadal spełniają Państwo warunki certyfikacji.

Przebieg wizyty

Tematy auditu kontrolnego zostały z Państwem uzgodnione zwykle podczas poprzedniej wizyty. Szczegóły zostaną ustalone na spotkaniu otwierającym.

Wybrane tematy auditu pozwolą nam na sprawdzenie:

- aktualnej oceny ryzyka i/lub zmian wprowadzonych w tym zakresie od czasu naszej poprzedniej wizyty
- procesu auditu wewnętrznego i przeglądu zarządzania
- raportowania zdarzeń i ich zarządzania
- postępu w realizacji celów i zadań doskonalących z zakresu bezpieczeństwa łańcucha dostaw
- działań korygujących i zapobiegawczych
- zmian wprowadzonych w systemie, ich wpływu na zarządzanie ryzykiem i skuteczność ich wdrożenia
- przestrzegania przepisów prawa i innych, do których spełniania się Państwo zobowiązaliście
- sposobu zarządzania zmianami zakresu obowiązków i kompetencji kluczowych pracowników

Sprawdzimy również działania korygujące podejmowane w stosunku do otwartych niezgodności oraz sposób wykorzystania logo LRQA i, tam, gdzie to właściwe, instytucji akredytacyjnej.

Jeżeli podczas naszej wizyty stwierdzimy jakieś Małe niezgodności, a termin kolejnej wizyty przypada za sześć miesięcy, to dokonamy oceny przeprowadzonych działań korygujących podczas tej wizyty. W innym przypadku uzgodnimy z Państwem termin wizyty dodatkowej, w przeciągu sześciu miesięcy.

Jeżeli podczas naszej wizyty stwierdzimy jakąś Większą Niezgodność, to przeprowadzimy dodatkowy audit kontrolny (zwykle w ciągu trzech miesięcy), aby sprawdzić podjęte przez Państwa działania korygujące. Jest to pierwszy krok w kierunku zawieszenia i wycofania naszej certyfikacji.

Jeżeli kolejna wizyta przypada w terminie odnowienia certyfikatu, nasz auditor dokona przeglądu zapisów związanych z tzw. „elementami systemowymi” systemu zarządzania, obejmującymi:

- historię szacowania ryzyka, najnowsze spostrzeżenia w tym zakresie oraz wpływ wszelkich zmian na system zarządzania
- przegląd zarządzania
- zarządzenie zmianą
- ciągłe doskonalenie
- audyty wewnętrzne
- działania korygujące
- działania zapobiegawcze
- nasze raporty z wizyt kontrolnych, oraz
- zmiany w Państwa systemie zarządzania.

Przegląd dotyczyć będzie bieżącego okresu certyfikacji (to znaczy ostatnich trzech lat) i zakończy się ustaleniem niezbędnego zakresu auditu, który należy przeprowadzić w celu odnowienia certyfikatu. Dlatego ważne jest, aby utrzymywali Państwo odpowiednie zapisy.

Na spotkaniu zamykającym nasz auditor podzieli się spostrzeżeniami ze swojej wizyty i ustali z Państwem temat kolejnego auditu. Jeżeli stwierdzono Większe niezgodności, to auditor ustali z Państwem również, wszelkie działania związane z przeglądem Państwa działań korygujących.

Raportowanie

Sposób sporządzania raportu z etapu 1 i etapu 2 oraz z auditu kontrolnego jest podobny. Wypełniamy formularze raportów, na których podajemy spostrzeżenia z przebiegu auditu, postęp w realizacji planu auditów, uwagi pozytywne, a także sprawy do wyjaśnienia. Spostrzeżenia z auditu wprowadzane są do Rejestru Spostrzeżeń z Auditów i klasyfikowane jako: Większa Niezgodność i Mniejsza Niezgodność. Definicje tych ocen znajdują Państwo poniżej:

Większa niezgodność: Wada systemu, która:

- ma już wpływ na skuteczność systemu lub rezultaty jego działania
- zagraża wydolności systemu zarządzania
- wymaga podjęcia natychmiastowego działania
- wymaga natychmiastowego przeprowadzenia analizy źródłowej przyczyny niezgodności i działań korygujących.

Auditor wiodący naszego zespołu auditorów ustali z Państwem szczegóły działań, które należy podjąć.

Mniejsza niezgodność: słabość procesów lub procedur wewnętrznych lub inne spostrzeżenie, które w – przypadku dalszej utraty kontroli – mogłoby spowodować nieskuteczność systemu. Wymaga analizy źródła niezgodności i działań korygujących.

Jeżeli Mniejsza niezgodność zostanie wykryta na 2 etapie certyfikacji lub w trakcie odnawiania certyfikatu, auditor poprosi o przedstawienie działań korygujących, które zamierzają Państwo podjąć. Ten plan działań korygujących będzie przedmiotem niezależnej analizy w naszym biurze, zanim certyfikat zostanie Państwu wydany. Jeżeli zaś niezgodność ta zostanie wykryta podczas auditu kontrolnego, to chociaż nadal muszą Państwo podjąć działania korygujące w odpowiednim terminie, najczęściej nie będzie konieczności przedstawiania nam szczegółów tych czynności do czasu naszej kolejnej wizyty.

W obu przypadkach, podczas kolejnej wizyty auditor zweryfikuje podjęte przez Państwa działania i wypełni część poświęconą działaniom korygującym w Rejestrze spostrzeżeń z auditu.

Kopie raportów należy przechowywać przez okres trzech lat. W wyjątkowych sytuacjach możemy Państwa poprosić o przedstawienie kopii wcześniejszych raportów.

Dobieranie próby

Należy pamiętać, że chociaż jakiś problem, dotyczący pewnej części Państwa działalności, nie został wykryty, nie oznacza to od razu, że takiego problemu nie ma. Audit prowadzony jest w oparciu o dobraną próbę i – statystycznie rzecz ujmując – zawsze występuje prawdopodobieństwo, że czegoś nie uda się wykryć. Należy o tym pamiętać zawsze, kiedy prowadzą Państwo audit wewnętrzny własnego systemu zarządzania.

Poufność

Żadne informacje dotyczące Państwa organizacji (w tym treść raportów) nie będą przez nas udostępniane żadnej innej osobie fizycznej lub prawnej bez Państwa zgody (z zastrzeżeniem wymogów instytucji akredytującej).

ISO 28003 zawiera szczegółowe informacje dotyczące poufności i bezpieczeństwa informacji oraz zwolnienia z obowiązku zachowania poufności dla auditorów i ekspertów.

LRQA korzysta z najwyższej jakości zabezpieczeń dotyczących bezpieczeństwa informacji wrażliwych o naszych klientach.

Akredytacja

LRQA jest w trakcie uzyskiwania akredytacji do wydawania certyfikatów ISO28000 dla systemów zarządzania bezpieczeństwem od Brytyjskiej Instytucji Akredytacyjnej UKAS.

Więcej informacji

Więcej informacji o tym, w jaki sposób LRQA może Państwu pomóc w spełnieniu wymogów branżowych i zachowaniu konkurencyjności, znajduje się na naszej stronie www.lrq.com. Znajdą tam Państwo więcej informacji o naszych usługach dotyczących bezpieczeństwa łańcucha dostaw i innych. Znajdują się tam również odnośniki do krajowych stron LRQA, na których podajemy informacje o działalności LRQA w Państwa kraju.

Staraliśmy się, aby informacje zawarte w tej „Informacji dla Klienta” były zgodne ze stanem faktycznym na dzień wydania. Wymagania, których dotyczy ten dokument, mogą się jednak zmieniać. W razie wątpliwości, prosimy o kontakt z najbliższym oddziałem naszej firmy, który udostępni Państwu aktualną wersję tego dokumentu.

Staraliśmy się, aby informacje zawarte w tej „Informacji dla Klienta” były zgodne ze stanem faktycznym na dzień wydania. Wymagania, których dotyczy ten dokument, mogą się jednak zmieniać. W razie wątpliwości, prosimy o kontakt z najbliższym oddziałem naszej firmy, który zapewni Państwu aktualną wersję tego dokumentu.

LRQA Polska
Ul. Grunwaldzka 12-16, lokal 1
81-759 Sopot
Tel.: 058 555 75 00, Fax 058 555 75 01
email: lrqa@lrqa.pl
www.lrq.pl

