Komunikat nr 115 z dnia 12.11.2012 r.

w sprawie wprowadzenia zmian w wymaganiach akredytacyjnych dla jednostek certyfikujących systemy zarządzania bezpieczeństwem informacji wynikających z opublikowania normy ISO/IEC 27006:2011

Informujemy o zmianie wymagań akredytacyjnych dla jednostek certyfikujących systemy zarządzania bezpieczeństwem informacji wg PN-ISO/IEC 27001.

1. Norma międzynarodowa ISO/IEC 27006:2007 *Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*, w prowadzona do zbioru Polskich Norm jako PN-EN ISO/IEC 27006:2009 *Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji,* została zastąpiona przez normę ISO/IEC 27006:2011.
2. Zgodnie z *Rezolucją IAF nr 2012-08* podjętą przez Zgromadzenie Ogólne IAF w dniach 24 i 26 października 2012 roku okres przejściowy związany z wdrożeniem normy ISO/IEC 27006:2011 przez akredytowane jednostki certyfikujące systemy zarządzania bezpieczeństwem informacji trwa do 01.06.2013 roku.
3. Po 1.06.2013 roku certyfikaty akredytacji jednostek certyfikujących systemy zarządzania bezpieczeństwem informacji wydane przez PCA w odniesieniu do wymagań normy PN-ISO/IEC 27006:2007 stracą ważność.
4. Od dnia publikacji niniejszego komunikatu oceny jednostek certyfikujących systemy zarządzania bezpieczeństwem informacji realizowane będą z uwzględnieniem wymagań ISO/IEC 27006:2011.
5. Procesy akredytacji według PN-ISO/IEC 27006:2007 będą kontynuowane według wymagań PN-ISO/IEC 27006:2007 pod warunkiem, że jednostka podda się dodatkowej ocenie w odniesieniu do znowelizowanych wymagań ISO/IEC 27006:2011 przed końcem wskazanego poniżej terminu wdrożenia.
6. Akredytowane jednostki certyfikujące systemy zarządzania bezpieczeństwem informacji są zobowiązane do wdrożenia wymagań znowelizowanej normy ISO/IEC 27006:2011 tak, aby możliwe było dokonanie oceny ich wdrożenia przed 1.06.2013 roku. Ocena wdrożenia wymagań ISO/IEC 27006:2011 będzie prowadzona podczas ocen na miejscu zgodnie z harmonogramem nadzoru lub w formie przeglądu dokumentacji jako dodatkowa ocena. Ocena wdrożenia wymagań znowelizowanej normy ISO/IEC 27006:2011 prowadzona będzie w zakresie zmienionych wymagań, przedstawionych w załączniku do niniejszego komunikatu.

D Y R E K T O R
POLSKIEGO CENTRUM AKREDYTACJI

dr inż. Eugeniusz W. Roguski

Porównanie treści normy ISO/IEC 27006:2007 (PN-ISO/IEC 27009:2009) i ISO/IEC 27006:2011		
Punkt	**ISO/IEC 27006:2007**	**ISO/IEC 27006:2011**
Cała norma	Wymagania z ISO/IEC 17021: 2009, Rozdział …, mają zastosowanie	Wymagania z ISO/IEC 17021: 2011, Rozdział …, mają zastosowanie
Przedmowa	Głównym zadaniem wspólnego komitetu technicznego jest przygotowanie Norm Międzynarodowych. Projekty Norm Międzynarodowych, przyjęte przez wspólny komitet techniczny, są przesyłane organizacjom członkowskim w celu przeprowadzenia głosowania. Publikacja w postaci Normy Międzynarodowej wymaga akceptacji co najmniej 75 % organizacji członkowskich biorących udział w głosowaniu.	Głównym zadaniem wspólnego komitetu technicznego jest przygotowanie Norm Międzynarodowych. Projekty Norm Międzynarodowych, przyjęte przez wspólny komitet techniczny, są przesyłane organizacjom krajowym w celu przeprowadzenia głosowania. Publikacja w postaci Normy Międzynarodowej wymaga akceptacji co najmniej 75 % organizacji krajowych biorących udział w głosowaniu.
Przedmowa	Brak treści.	Drugie wydanie normy unieważnia i zastępuje wydanie pierwsze normy (ISO/IEC 27006:2007), które zostało zweryfikowane pod względem technicznym.
Wprowadzenie	ISO/IEC 17021 jest Normą Międzynarodową, w której ustalono kryteria dla jednostek prowadzących audyt i certyfikację systemów zarządzania organizacji.	ISO/IEC 17021 ustala kryteria dla jednostek prowadzących audyt i certyfikację systemów zarządzania organizacji.
Wprowadzenie	Termin „zaleca się" jest stosowany do wskazania tych postanowień, co do których, chociaż stanowią wytyczne do stosowania wymagań, oczekuje się, że zostaną zastosowane przez jednostkę certyfikującą.	Termin „zaleca się" jest stosowany do wskazania postanowień zalecanych.
Wprowadzenie	Jedynym celem niniejszej Normy Międzynarodowej jest umożliwienie jednostkom akredytacyjnym efektywniejszego harmonizowania zastosowania norm ze swoim zobowiązaniem do oceniania jednostek certyfikujących. W tym przypadku każde odstępstwo jednostki certyfikującej od wytycznych to wyjątek. Takie odstępstwa są dopuszczalne tylko w konkretnym przypadku, po zademonstrowaniu przez jednostkę certyfikującą jednostce akredytującej, że wyjątek w pewien sposób stanowi równoważne podejście do odpowiednich rozdziałów wymagań z ISO/IEC 17021, ISO/IEC 27001 oraz celów niniejszej Normy Międzynarodowej.	Jedynym celem niniejszej Normy Międzynarodowej jest umożliwienie jednostkom akredytacyjnym efektywniejszego harmonizowania zastosowania norm ze swoim zobowiązaniem do oceniania jednostek certyfikujących.

5.2.1.c	c) udostępnienie lub publikacja na żądanie informacji opisującej interpretację jednostki certyfikującej wymagań standardów audytu certyfikacyjnego;	c) udostępnienie lub publikacja na żądanie informacji opisującej interpretację jednostki certyfikującej wymagań standardów audytu certyfikacyjnego (patrz punkt 9.1.1.1);
5.2.1.d	Wersja Polska bez zmian (zaleca się) Wersja angielska „should" – „powinien" czyli „ma obowiązek".	Wersja Polska bez zmian (zaleca się) Wersja angielska „shall" – „zaleca się".
7.1.2	Brak punktu.	7.1.2 IS 7.1.2 Określanie kryteriów kompetencji. Dodatkowe informacje dotyczące wiedzy i umiejętności, są zamieszczone w Załączniku B jako uzupełnienie kryteriów z ISO/IEC 17021.
7.2.1.3.2.a	Mieć wiedzę i cechy potrzebne do zarządzania procesem audytu certyfikacyjnego;	Mieć wiedzę i umiejętności potrzebne do zarządzania procesem audytu certyfikacyjnego
8.1.1	Jednostka certyfikująca powinna dysponować udokumentowanymi procedurami dla: a) audytu certyfikacyjnego SZBI organizacji klienta, zgodnie z postanowieniami ISO 19011, ISO/IEC 17021 i innych związanych dokumentów; b) okresowych audytów w nadzorze i audytów odnowienia certyfikacji SZBI organizacji klienta zgodnie z ISO 19011 i ISO/IEC 17021, opierających się na ciągłym potwierdzaniu odpowiednich wymagań oraz weryfikacji i zapisywaniu, że organizacja klienta prowadzi w odpowiednim czasie działania korygujące dla usunięcia wszystkich niezgodności.	Jednostka certyfikująca powinna dysponować udokumentowanymi procedurami dla: a) audytu certyfikacyjnego SZBI organizacji klienta, zgodnie z postanowieniami ISO/IEC 17021 i innych związanych dokumentów; b) okresowych audytów w nadzorze i audytów odnowienia certyfikacji SZBI organizacji klienta zgodnie z ISO/IEC 17021, opierających się na ciągłym potwierdzaniu odpowiednich wymagań oraz weryfikacji i zapisywaniu, że organizacja klienta prowadzi w odpowiednim czasie działania korygujące dla usunięcia wszystkich niezgodności.
8.2.1	Brak uwagi.	UWAGA: Zmiany w Deklaracji Stosowania, które nie wpływają na zmianę zakresu certyfikacji nie wymagają wydania nowego certyfikatu.
9.1.3	Jednostki certyfikujące powinny zapewnić audytorom wystarczający czas do przeprowadzenia wszystkich działań związanych z audytem certyfikacyjnym, audytami w nadzorze i audycie odnowienia. Zaleca się, żeby przydzielony czas opierał się na takich czynnikach jak:	Jednostki certyfikujące powinny zapewnić audytorom wystarczający czas do przeprowadzenia wszystkich działań związanych z audytem certyfikacyjnym, audytami w nadzorze i audycie odnowienia. Przydzielony czas powinien uwzględniać następujące czynniki:
9.1.4.2.e	Program nadzoru został opracowany pod kątem powyższych	Program auditu został opracowany pod kątem powyższych

	wymagań i w rozsądnym czasie objął wszystkie lokalizacje organizacji klienta w zakresie SZBI.	wymagań i obejmuje reprezentatywne próbki z zakresu certyfikacji ISMS w okresie trzech lat.
9.1.6.1	Jednostka certyfikująca może zaadaptować procedury raportowania, które spełniają jej potrzeby, ale jako minimum procedury te powinny zapewniać, że:	Procedury raportowania jednostki certyfikującej powinny zapewniać, że:
9.1.6.2	Zaleca się, aby raport z audytu zawierał następujące informacje:	Raport z audytu powinien zawierać następujące informacje lub się do nich odnieść:
9.1.6.3	Spostrzeżenia zawarte w raporcie z audytu dostarczone do organizacji certyfikującej powinny być wystarczająco dokładne dla ułatwienia i wspierania decyzji o certyfikacji oraz powinny dotyczyć:	Raport z audytu powinien być wystarczająco dokładny dla ułatwienia i wspierania decyzji o certyfikacji oraz powinien dotyczyć:
9.1.6.3.c	c) szczegółów wykrytych niezgodności, popartych obiektywnymi dowodami, i odniesienia tych niezgodności do wymagań dotyczącej SZBI normy ISO/IEC 27001 lub innych dokumentów wymaganych do certyfikacji;	c) szczegółów wykrytych niezgodności, popartych obiektywnymi dowodami, i odniesienia tych niezgodności do wymagań dotyczącej normy ISO/IEC 27001 lub innych dokumentów wymaganych do certyfikacji;
IS 9.2.3.1	Pierwszy etap audytu obejmuje przegląd dokumentów, ale zaleca się, aby nie ograniczał się tylko do tego.	Pierwszy etap audytu powinien obejmować przegląd dokumentów, ale zaleca się, aby nie ograniczał się tylko do tego.
9.2.3.3.3	UWAGA ISO 19011 dostarcza wytycznych do prowadzenia połączonych audytów systemów zarządzania.	Usunięto uwagę.
9.3.1.1	Procedury audytu w nadzorze powinny być spójne z tymi, które dotyczą audytu certyfikacyjnego SZBI organizacji klienta, jak to przedstawiono w niniejszej normie.	Procedury audytu w nadzorze powinny być spójne z tymi, które dotyczą audytu certyfikacyjnego SZBI organizacji klienta, jak to przedstawiono w niniejszej międzynarodowej normie.
9.3.1.3	Zaleca się, żeby nadzór jednostki certyfikującej obejmował przynajmniej punkty wymagane dla audytu w nadzorze w ISO/IEC 17021. Dodatkowo zaleca się, żeby następujące zagadnienia zostały wzięte pod uwagę. a) Zaleca się, żeby jednostka certyfikująca była w stanie dostosować swój program nadzoru do zagadnień bezpieczeństwa informacji związanych z zagrożeniami dla aktywów, podatnościami oraz skutkami dla organizacji klienta i uzasadnić ten program.	Nadzór jednostki certyfikującej powinien obejmować przynajmniej punkty wymagane dla audytu w nadzorze w ISO/IEC 17021. Dodatkowo zaleca się, żeby następujące zagadnienia zostały wzięte pod uwagę. a) Jednostka certyfikująca powinna być w stanie dostosować swój program nadzoru do zagadnień bezpieczeństwa informacji związanych z zagrożeniami dla aktywów, podatnościami oraz skutkami dla organizacji klienta i uzasadnić ten program.

	b) Zaleca się, aby program nadzoru jednostki certyfikującej był ustalany przez jednostkę certyfikującą. Konkretne daty wizyt mogą być uzgadniane z certyfikowaną organizacją klienta. d) Jednostka certyfikująca jest zobowiązana do nadzorowania właściwego korzystania z certyfikatu.	b) Program nadzoru jednostki certyfikującej powinien być ustalany przez jednostkę certyfikującą. Konkretne daty wizyt mogą być uzgadniane z certyfikowaną organizacją klienta. d) Jednostka certyfikująca powinna nadzorować właściwe korzystanie z certyfikatu.
9.5.1	Działania w nadzorze powinny podlegać szczególnym postanowieniom, jeśli organizacja klienta z wdrożonym SZBI wykonuje duże modyfikacje swojego systemu lub jeżeli miały miejsce inne zmiany mogące wpłynąć na podstawę jej certyfikacji.	Działania potrzebne do przeprowadzenia auditów specjalnych powinny podlegać szczególnym postanowieniom, jeśli organizacja klienta z wdrożonym SZBI wykonuje duże modyfikacje swojego systemu lub jeżeli miały miejsce inne zmiany mogące wpłynąć na podstawę jej certyfikacji.
Tabela A.1	Brak podpisu pod Tablicą A.1 – Kryteria określania złożoności SZBI.	Liczby w tabeli podano jedynie jako wartości przykładowe. Zaleca się, by jednostki certyfikujące same określiły odpowiednie wartości.
B.1	Istnieje kilka sposobów potwierdzenia przez audytora jego wiedzy i doświadczenia. Wiedzą i doświadczeniem można się wykazać, na przykład, poprzez wykorzystanie uznanych kwalifikacji. Rejestracja np. wg wymagań IRCA, lub jakakolwiek inna uznana forma rejestracji audytora może także być wykorzystana do zademonstrowania wymaganej wiedzy i doświadczenia.	Istnieje kilka sposobów potwierdzenia przez audytora jego wiedzy i doświadczenia. Wiedzę i doświadczenie można ocenić, na przykład, poprzez wykorzystanie uznanych kwalifikacji. Rejestracja zapisów zgodnych ze schematem certyfikacji personelu może również zostać wykorzystana do sprawdzenia wymaganej wiedzy i doświadczenia.