Komunikat nr 145 z dnia 6.06.2014 r.

w sprawie okresu przejściowego związanego z opublikowaniem ISO/IEC 27001:2013

Informujemy, że z dniem 1.10.2013 r. opublikowana została norma ISO/IEC 27001:2013 *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.*

Zgodnie z *Rezolucją IAF nr 2013-12* podjętą przez Zgromadzenie Ogólne IAF w dniach 23 i 25 października 2013 roku termin osiągnięcia zgodności z normą ISO/IEC 27001:2013 określono na **2 lata od jej publikacji.** W związku z powyższym, ostateczną datą przejścia akredytowanych jednostek certyfikujących systemy zarządzania bezpieczeństwem informacji (ISMS) na przedmiotową normę jest 1.10.2015 r.

Jednocześnie zgodnie z ww. Rezolucją, w rok po opublikowaniu ISO/IEC 27001:2013, wszystkie nowe akredytowane certyfikaty w obszarze ISMS powinny być wydawane na zgodność z ISO/IEC 27001:2013.

Poniżej przedstawiono zasady postępowania PCA w okresie przejściowym.

CAB w procesie akredytacji	Procesy akredytacji jednostek certyfikujących systemy zarządzania bezpieczeństwem informacji nie zakończone **do 1.10.2014** roku będą kontynuowane pod warunkiem, że wnioskujący podmiot wykaże swoje kompetencje do certyfikacji w odniesieniu do nowej normy ISO/IEC 27001:2013.
akredytowane CAB - w trakcie nadzoru	**Od dnia 1.07.2014 r**. oceny na miejscu w jednostkach posiadających akredytację w obszarze ISMS, prowadzone zgodnie z harmonogramem nadzoru, będą obejmować kompetencje CAB do nowej normy. Akredytowane jednostki certyfikujące systemy zarządzania bezpieczeństwem informacji są zobowiązane do: a) odpowiedniego przeszkolenia swoich auditorów w odniesieniu do wymagań normy ISO/IEC 27001:2013; b) dostosowania swoich wymagań kompetencyjnych do nowej normy, szczególnie w obszarze „kompetencji technicznych"; c) określenia dla swoich klientów planu przejścia z normy ISO/IEC 27001:2005 na ISO/IEC 27001:2013 tak, aby wszystkie istniejące certyfikaty zostały wydane na nową normę przed 1.10.2015 r.; d) dostosowania swoich metod działania (instrukcje, szablony, listy kontrolne) do nowych wymagań. Podczas obserwacji działań jednostki w programie ISMS, PCA szczególną uwagę zwróci na odpowiednią metodę oceny: „analizy ryzyka", „deklaracji stosowania", „polityki bezpieczeństwa informacji" Poza oceną w planowanym nadzorze, na życzenie CAB, możliwa jest dodatkowa ocena na miejscu celem potwierdzenia kompetencji do nowej

	normy ISO/IEC 27001:2013. Alternatywą dla takiej dodatkowej oceny w siedzibie jest przesłanie przez CAB dowodów na zrealizowanie działań określonych w punktach a) do d) i ocena tych dowodów przez PCA w ramach przeglądu dokumentacji.

D Y R E K T O R
POLSKIEGO CENTRUM AKREDYTACJI

dr inż. Eugeniusz W. Roguski