PRS Certyfikacja

**Nowe wydanie normy ISO/IEC 27001:2013**

25 września 2013 została opublikowana przez Międzynarodową Organizację Normalizacyjną (ISO) i Międzynarodową Komisję Elektrotechniczną (IEC) norma ISO/IEC 27001:2013 – „Technologie informatyczne - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania”). Nowe wydanie normy zastępuje i unieważnia poprzednie wydanie normy ISO/IEC 27001:2005.

Nowe wydanie normy ma następującą strukturę:

1. Zakres normy
2. Postanowienia ogólne
3. Terminy i definicje
4. System zarządzania bezpieczeństwem informacji
5. Przywództwo bezpieczeństwa informacji i wsparcie na wysokim poziomie w zakresie polityki bezpieczeństwa
6. Planowanie SZBI, ocena ryzyka, postępowanie z ryzykiem
7. Wspieranie SZBI
8. Sterowanie operacyjne SZBI
9. Przegląd wydajności SZBI
10. Doskonalenie SZBI

Załącznik A: Zabezpieczenia i cele zabezpieczeń

Załączniki B i C z wydania 2005 zostały usunięte.

Załącznik A został przebudowany i obecnie wskazuje 114 zabezpieczeń w 14 grupach:

- A.5 Polityka bezpieczeństwa informacji
- A.6 Organizacja bezpieczeństwa informacji
- A.7 Bezpieczeństwo zasobów ludzkich (przed, w trakcie i po okresie zatrudnienia)
- A.8 Zarządzanie aktywami
- A.9 Kontrola dostępu
- A.10 Kryptografia
- A.11 Bezpieczeństwo fizyczne i środowiskowe
- A.12 Bezpieczeństwo operacyjne
- A.13 Bezpieczeństwo łączności
- A.14 Zakup systemu, rozwój i utrzymanie
- A.15 Relacje z dostawcami
- A.16 Zarządzanie incydentami bezpieczeństwa
- A.17 Bezpieczeństwo informacji zarządzania ciągłością działania
- A.18 Zgodność z wymaganiami (wewnętrznymi takimi jak polityka i zewnętrznymi takimi jak wymagania prawne)

W załączniku A pojawiły się nowe elementy sterujące:

- A.6.1.5 Bezpieczeństwo informacji w zarządzaniu projektami
- A.12.6.2 Ograniczenia dotyczące instalacji oprogramowania
- A.14.2.1 Polityka bezpiecznego rozwoju
- A.14.2.5 System bezpiecznych zasad inżynieryjnych
- A.14.2.6 Bezpieczne środowisko programistyczne
- A.14.2.8 Testowanie systemu bezpieczeństwa
- A.15.1.1 Polityka bezpieczeństwa informacji dla relacji z dostawcami
- A.151.3 Informacja i komunikacja w łańcuchu dostaw technologii
- A16.1.4 Ocena i decyzja w sprawie bezpieczeństwa imprez informacyjnych
- A.16.1.5 Reakcja na incydent bezpieczeństwa informacji
- A.17.2.1 Dostępność infrastruktury przetwarzania informacji

Przyjęta struktura normy miała na celu jej ujednolicenie w stosunku do innych norm dot. systemów zarządzania, takich jak ISO/IEC 22301:2012 (zarządzanie ciągłością działania), ISO/IEC 20000-1:2011 (zarządzanie usługami IT) czy opracowywanego nowego wydania normy ISO 9001:2014. Podobna struktura poszczególnych norm ma pomóc organizacjom w lepszym stosowaniu zintegrowanych polityk oraz procedur. Nowa norma ma także przygotować SZBI do pojawiających się nowych technologii informatycznych, np. „chmura" oraz do współczesnych zagrożeń, takich jak kradzież tożsamości, ryzyko związane z telefonami komórkowymi oraz innymi słabościami technologii online.

Nowa norma kładzie nacisk na pomiar i ocenę skuteczności SZBI, a także na wykorzystywanie outsourcingu w wielu aspektach działalności coraz to szerszej grupy organizacji. Norma nie koncentruje się tak mocno na zasadzie Zaplanuj-Wykonaj-Sprawdź-Działaj. Większy nacisk położony jest na organizacyjne aspekty bezpieczeństwa i ocenę ryzyka. Norma wprowadza podejście do zarządzania ryzykiem oparte na ISO/IEC 31000:2009, które zezwala na bardziej miękkie podejście do analiz niż prezentowane w ISO/IEC 27005:2008.

Opracował: Michał Gałecki, auditor wiodący Polskiego Rejestru Statków S.A. w zakresie systemów zarządzania bezpieczeństwem informacji ISO 27001, zarządzania jakością ISO 9001, zarządzania środowiskowego ISO 14000, zarządzania bezpieczeństwem i higieną pracy PN-N-18001 i OHSAS oraz zarządzania jakością w motoryzacji ISO/TS 16949.