

Samodzielny audit z zakresu ochrony danych osobowych oraz przygotowanie do kontroli z Biura Generalnego Inspektora Ochrony Danych Osobowych



**Wykładowca – mgr prawa i mgr inż. elektronik
Wacław Zimny**

- stosowane obie formy audyt i audytor są poprawne - Praktyczny Słownik Współczesnej Polszczyzny wydawnictwa Kurpisz z 1994 roku.

- 4.1.007 **audyt** zabezpieczenia systemu - dokonanie niezależnego przeglądu i **oceny** (4.1.044) działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się, czy system działa zgodnie z ustaloną **polityką zabezpieczenia** (4.1.065) i procedurami operacyjnymi oraz w celu wykrycia **przełamania** **zabezpieczenia** (4.1.075) i zalecenia wskazanych zmian w środkach nadzorowania, polityce zabezpieczenia oraz procedurach

audit

(PrPN-I-02000 Technika informatyczna Zabezpieczenia w systemach informatycznych Terminologia 1999r.)

- **FINANSOWY** ustanowiony ustawą z dnia 26 listopada 1998 r. o finansach publicznych (Dz. U. z 1998r. Nr 155, poz. 1014) oraz Rozporządzeniem Ministra Finansów z dnia 5 lipca 2002 r. w sprawie szczegółowego sposobu i trybu przeprowadzania audytu wewnętrznego (Dz. U. z 2002r. Nr 111, poz. 973),
- **ENERGETYCZNY** ustanowiony Rozporządzeniem Ministra Infrastruktury z dnia 15 stycznia 2002 r. w sprawie szczegółowego zakresu i formy audytu energetycznego (Dz. U. z 2002r. Nr 12, poz. 114),
- **EKOZARZĄDZANIA** ustanowiony ustawą z dnia 12 marca 2004 r. o krajowym systemie ekozarządzania i audytu (EMAS) (Dz. U. 2004 r. Nr 70, poz.631).

Pojęcie „**audytu**” wyszło poza ramy przepisów prawa i zrobiło oszałamiającą karierę w relacjach nieskodyfikowanych.

Termin „**audyt**” jest obecnie używany nieomal w każdej dziedzinie **w znaczeniu kształtowanym zwyczajowo** w tych dziedzinach!

Cechą wspólną powszechnego użycia pojęcia „**audytu**” jest postrzeganie go jako określonej formy badania stanu (kontroli) usługi/produktu audytowanego przez podmiot z odpowiednimi kwalifikacjami, zakończonego zazwyczaj sprawozdaniem.

Czego najczęściej dotyczą nieskodyfikowane audyty? – np.:

- firmowych **podatków**,
- kadry pracowniczej (audyt **personalny** lub **kompetencyjny**) pozwala określić potencjał kadry w przedsiębiorstwie, zbadać potrzeby szkoleniowe, planować ścieżki kariery oraz tworzyć rezerwy kadrowe,
- **logistyki** (pozwala ocenić sprawność i efektywność procesów logistycznych w obszarze magazynowania, zarządzania zapasami, transportu, dystrybucji i zaopatrzenia na poziomie strategicznego zarządzania przedsiębiorstwem),
- **komunikacji** (pomaga m.in. zdefiniować zatory i interferencje komunikacyjne oraz nadmierny szum informacyjny),
- **IT** (działanie prowadzone przez osobę lub grupę osób spoza grona wykonawczego określonego przedsięwzięcia informatycznego),
- **systemów komputerowych** (audytorem powinna być osoba, która nie brała udziału w instalacji systemu, gdyż zakłada się, że administrator instalujący system operacyjny nie jest w stanie sam obiektywnie ocenić jego bezpieczeństwa),
- inwentaryzacji, stopnia wykorzystania i legalności posiadanego **oprogramowania**,
- poprawności **usług** świadczonych drogą elektroniczną,
- przedsięwzięć **teleinformatycznych**, a w tym **ochrony danych osobowych**.

nie należy mylić auditu z certyfikacją!

USTAWA z dnia 30 sierpnia 2002 r. **o systemie oceny zgodności** (Dz. U. z dnia 7 października 2002 Nr 166, poz. 1360) kreuje :

- 2) zasady funkcjonowania systemu oceny zgodności z zasadniczymi i szczegółowymi wymaganiami dotyczącymi wyrobów;
- 3) zasady i tryb udzielania akredytacji oraz autoryzacji;
- 4) sposób zgłaszania Komisji Europejskiej i państwom członkowskim Unii Europejskiej autoryzowanych jednostek oraz autoryzowanych laboratoriów;
- 5) zadania Polskiego Centrum Akredytacji;
- 6) zasady działania systemu kontroli wyrobów wprowadzonych do obrotu.

Art. 15. 1. Akredytacja jest udzielana przez **Polskie Centrum Akredytacji**, na wniosek zainteresowanej **jednostki certyfikującej, jednostki kontrolującej, laboratorium** lub innego **podmiotu przeprowadzającego oceny zgodności lub weryfikacje**, **po potwierdzeniu, że spełniają wymagania i warunki określone w odpowiednich Polskich Normach, a w przypadku braku PN - w odpowiednich dokumentach organizacji międzynarodowych.**

Art. 3. System oceny zgodności tworzą:

- 9) przepisy określające zasadnicze i szczegółowe wymagania dotyczące wyrobów;
- 10) przepisy oraz normy określające działanie uczestniczących w procesie oceny zgodności.

Art. 8. 1. Producent lub jego upoważniony przedstawiciel, który poddał wyrób lub proces jego wytwarzania ocenie zgodności z zasadniczymi wymaganiami i potwierdził ich zgodność, wystawia deklarację zgodności lub umieszcza oznakowanie CE, zgodnie z wymaganiami określonymi w dyrektywach nowego podejścia.

typowy audyt polityki bezpieczeństwa

Audyt polityki bezpieczeństwa

- Specyfikacja infrastruktury informatycznej organizacji.
- Specyfikacja zastosowanych zabezpieczeń.
- Ocena założeń koncepcyjnych stosowanych zabezpieczeń.
- Ocena wyboru zastosowanych procedur zabezpieczeń.
- Ocena wyboru zastosowanych technik i narzędzi.
- Analiza rutynowych procedur obsługi systemu zabezpieczeń.
- Analiza procedur reakcji na incydenty.

Audyt technicznych aspektów zabezpieczeń

- Specyfikacja architektury firewall, komponenty architektury, ich zadania i wzajemne interakcje.
- Specyfikacja kontrolowanej przez architekturę firewall komunikacji, określenie komunikacji dozwolonych i zabronionych.
- Ocena polityki inspekcji ruchu sieciowego, ocena zgodności zdefiniowanych konfiguracji z polityką inspekcji ruchu.
- Specyfikacja konfiguracji zastosowanych serwerów. Ekspertyza systemu operacyjnego, opracowanie zaleceń dotyczących ew. hardeningu systemu.
- Analiza bezpieczeństwa wymiany informacji z siecią wewnętrzną.
- Analiza bezpieczeństwa wymiany informacji z Internetem. Ekspertyza systemu operacyjnego, opracowanie zaleceń dotyczących ew. hardeningu systemu.
- Ocena zabezpieczeń aplikacji / bazy danych.

Poniższe pozycje należy uwzględnić przy samodzielnym audicie bezpieczeństwa przetwarzania danych osobowych

- Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji PN-ISO/IEC 17799
- Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania PN-I-07799-2
- Strona internetowa GODO: www.godo.gov.pl
 - ⊙ Ochrona prywatności w systemach teleinformatycznych
 - ⊙ Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym
 - ⊙ Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa