Standardy typu „best practice”

Artur Sierszeń
asiersz@kis.p.lodz.pl
http://bzyczek.kis.p.lodz.pl

Standardy w audycie

- Do standardów opracowanych przez odpowiednie organizacje dotyczących audytu należą:
  - ISO (*International Standard Organization*),
  - BSI (*British Standard Institute*)

ISO (*International Standard Organization*)

- ISO (*International Standard Organization*), powstała w 1947r i zrzesza różne organizacje standaryzacyjne. W ramach IEC (*International Electrotechnical Commision*) pracę nad standardami zarządzania bezpieczeństwem prowadzi podkomitet ISO/IEC JTC1/SC27.
- ISO/IEC 27001 to jedyna poddawana audytom norma międzynarodowa, która określa wymogi dotyczące systemów zarządzania bezpieczeństwem informacji (ISMS). Norma ta została opracowana w celu zapewnienia wyboru adekwatnych i proporcjonalnych środków bezpieczeństwa.

BSI (*British Standard Institute*)

- najstarsza organizacja standaryzacyjna z 1901r, która opracowała ponad 20.000 standardów. Brytyjski standard opracowany przez BSI i opisujący system zarządzania usługami informatycznymi składa się z dwóch części:
  - BS15000-1, która jest zbiorem wymagań, których spełnienie pozwala organizacji potwierdzić certyfikatem jakość swojego systemu zarządzania.
  - BS15000-2, druga część stanowi zbiór wytycznych, które podpowiadają sposób realizacji przedstawionych wymagań

BSI (*British Standard Institute*)

- W grudniu 2005r BS 15000 został zastąpiony międzynarodową normą ISO/IEC 20000:2005, która również składa się z dwóch części:
  - ISO/IEC 20000-1:2005, IT Service Management. Specyfication of IT Service Management
  - ISO/IEC 20000-2:2005, IT Service Management. Code of Practice for IT Service Management

Standardy typu best practice

- Zbiór zaleceń (najlepszych praktyk), które na podstawie doświadczenia innych osób, firm, wskazują najwłaściwszy sposób postępowania, osiągnięcia określonego celu.
- Czas osiągnięcia celu jest dużo krótszy niż wynosiłby czas opracowania własnych technik.

Standardy typu best practice

- Proces formułowania i wdrażania najlepszych praktyk jest wieloetapowy:
  - **złota myśl** – jeszcze nie poparta danymi, ale intuicyjnie wydaje się dobra, wymaga dalszej analizy
  - **dobra praktyka** – była już wdrożona i udowodniono jej słuszność, poparta danymi zebranymi w ramach jednego przypadku zastosowania
  - **lokalna najlepsza praktyka** – określono ją jako najlepsze podejście dla pewnych działów organizacji, w oparcio o dane z analizy wydajności procesów
  - **przemysłowa najlepsza praktyka** – najlepsze podejście dla całej organizacji, w oparciu o dane pochodzące z testów porównawczych wewnątrz i na zewnątrz organizacji.

Standardy ISACA.

- Mają za cel informować audytorów o minimalnym poziomie świadczonych usług, oraz firmy o poziomie oczekiwań w stosunku do audytora.
- Cechuje je zwięzły charakter i hierarchiczna struktura. W skład jej wchodzą trzy grupy dokumentów:
  - Standardy – jako obowiązkowe wymagania wobec postawy audytora i raportów audytowych,
  - Wytyczne, które mówią jak te standardy stosować oraz
  - Procedury, którymi są dokumenty o charakterze poglądowym, dostarczające przykładów, jak spełniać standardy w trakcie działań audytowych.
- Standardy te opisują statut audytu, niezależność, standardy i etykę zawodową, kompetencje, planowanie, wykonywanie prac audytowych, raportowanie i dalszy ciąg działań.

Norma PN-ISO/IEC 17799

- Stanowi zbiór wskazówek dla wdrożenia i utrzymania bezpieczeństwa informacji w instytucji lub przedsiębiorstwie. Rozdziały normy poświęcone konkretnym zagadnieniom wraz z wskazanymi celami opisuję poniżej.
- polityka bezpieczeństwa – Celem jej jest zapewnienie kierunków działania i wsparcia kierownictwa dla bezpieczeństwa informacji
- organizacja bezpieczeństwa – Celem jest zarządzanie bezpieczeństwem informacji wewnątrz instytucji
- klasyfikacja i kontrola aktywów – Utrzymanie odpowiedniej ochrony aktywów instytucji oraz zapewnienie właściwego poziomu ochrony aktywów informacyjnych.
- bezpieczeństwo osobowe – Ograniczenie ryzyka błędu ludzkiego, kradzieży, oszustwa lub niewłaściwego użytkowania zasobów
- bezpieczeństwo fizyczne i środowiskowe – Zapobieganie utracie, uszkodzeniu lub innym naruszeniom bezpieczeństwa aktywów oraz przerwaniu działalności biznesowej oraz zapobieganie ujawnieniu lub kradzieży informacji i urządzeń do przetwarzania informacji

Norma PN-ISO/IEC 17799

- zarządzanie systemami i sieciami – Zapewnienie poprawnego i bezpiecznego działania urządzeń do przetwarzania informacji, minimalizowanie ryzyka awarii systemów oraz zabezpieczenie integralności oprogramowania i informacji.
- kontrola dostępu do systemu – Kontrola dostępu do informacji biznesowych, oraz zapobieganie nieuprawnionemu dostępowi do systemów informatycznych.
- rozwój i utrzymanie systemu – Zapewnienie, że bezpieczeństwo jest wbudowane w systemy informacyjne
- zarządzanie ciągłością działania – Przeciwdziałanie przerwom w działalności biznesowej oraz ochrona krytycznych procesów biznesowych przed rozległymi awariami lub katastrofami.
- zgodność – Unikanie naruszania jakichkolwiek przepisów prawa karnego lub cywilnego, zobowiązań wynikających z ustaw, zarządzeń lub umów i jakichkolwiek wymagań bezpieczeństwa
- zgodność z polityką bezpieczeństwa
- rozważania dotyczące audytu systemu – Maksymalizowanie efektywności i minimalizowanie ingerencji w proces audytu systemu.

GMITS (*Guidelines fot the Management of IT Security*)

- seria norm ISO/IEC 13335. Zawiera pięć części raportu:
  - TR ISO/IEC 13335-1:1996 lub PN-I-1335-1:1999. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych.
  - TR ISO/IEC 13335-2:1997. Planowanie i zarządzanie bezpieczeństwem systemów informatycznych.
  - TR ISO/IEC 13335-3. Techniki zarządzania bezpieczeństwem systemów informatycznych.
  - TR ISO/IEC 13335-4. Wybór zabezpieczeń.
  - TR ISO/IEC 13335-5. Zabezpieczenie dla połączeń z sieciami zewnętrznymi.

NIST (*National Institute of Standards and Technology*)

- Narodowy Instytut Standaryzacji i Technologii to amerykańska agencja federalna, prowadząca działalność standaryzującą rozwiązania dla systemów informatycznych.
- Najważniejsze zalecenia publikacji NIST 800 – 14 Rekomendowane praktyki i reguły w zabezpieczaniu systemów informatycznych

NIST (*National Institute of Standards and Technology*)

można podzielić na kategorie:

- bezpieczeństwo proceduralne
- bezpieczeństwo używania Internetu
- bezpieczeństwo korzystania z poczty elektronicznej
- bezpieczeństwo korzystania z komputera
- bezpieczeństwo osobowe
- procedury zapewniające odtworzenie stanu normalnego danych i funkcjonowania systemów
- bezpieczeństwo fizyczne
- bezpieczeństwo sprzętu i oprogramowania

GAISP (*Generally Accepted Information Security Project*)

- Ogólnie przyjęte zasady bezpieczeństwa informacji
- Jest to projekt zmierzający do formułowania uniwersalnych zasad bezpieczeństwa informacji.
- Opiera się o standardy i dokumentacje:
  - Detailed Principles – STROWMAN, Common Body of Knowledge,
  - Standards of Good Practice for Information Security,
  - normę ISO 17799,
  - Control Objectives for Information Technology
  - Generally Accepted Principles and Practices for Securing Information Technology Systems.
- Treść GAISP dzieli się na dwie grupy, zawierające zasady podzielone wg. kryteriów:
  - zasady szerzenia (pervasive principles –PP)
  - zasady funkcjonalne (broad functional principles – BFP)

Zasady szerzenia (pervasive principles –PP)

- zasada rejestrowania dostępu do danych
- zasada świadomości
- zasada etyki
- zasada wielodyscyplinarna
- zasada integracji
- zasada aktualności
- zasada oceny
- zasada sprawiedliwości

Zasady funkcjonalne (broad functional principles – BFP)

- polityka bezpieczeństwa informacji
- edukacja i uświadamianie
- monitorowanie aktywności
- zarządzanie zasobami informacyjnymi
- zarządzanie środowiskowe
- kwalifikacje personalne
- zarządzanie incydentami
- cykl życia systemów informatycznych
- kontrola dostępu
- planowanie ciągłości operacyjnej i działania w sytuacji wyjątkowej
- zarządzanie ryzykiem zagrożeń informacji
- bezpieczeństwo sieciowe i internetowe
- prawne, regulacyjne i umowne aspekty bezpieczeństwa informacji
- praktyki etyczne

ITIL (*Information Technology Infrastructure Library*)

- kodeks postępowania dla działów informatyki. Jest to zbiór zaleceń, jak efektywnie i skutecznie oferować usługi informatyczne.
- ITIL dostarcza szeroki zestaw najlepszych praktyk wypracowanych przez sektor publiczny i firmy prywatne z całego świata, powszechnie stosowanych, aktywnie wspieranych przez ośrodki szkoleniowe i egzaminacyjne, dostawców usług informatycznych, wewnętrzne działy IT, dostawców narzędzi dla informatyki, klientów i użytkowników usług informatycznych oraz przez firmy doradcze.
- ITIL jest zarejestrowanym znakiem towarowym OGC (Office of Government Commerce).

ITIL (*Information Technology Infrastructure Library*)

- Obecnie dostępna jest trzecia wersja biblioteki ITIL opublikowana w 2007, składająca się z 5 publikacji.
- Service Strategy (Strategia Usług)
- Service Design (Projektowanie Usług)
  - Service Transition (Wdrażanie Usług)
  - Service Operation (Eksploatacja Usług)
  - Continual Service Improvement (Ciągła Poprawa Usług)
- ITIL to zbiór kompleksowych rekomendacji branży informatycznej, z których powstała międzynarodowa norma zarządzania usługami informatycznymi – ISO/IEC 20000 Service Management.

NRIC (*Network Reliability and Interoperability Council*)

- Departament ds. niezawodności i kompatybilności sieci.
- NRIC wspólnie z organizacjami uczestniczącymi w pracach nad bezpieczeństwem sieci (Cisco, Alcatel, Ericsson, AT&T, Lucent Technologies, Lockheed Martin, Motorola, Nokia i inni)
- zaproponował zbiór najlepszych praktyk z zakresu bezpieczeństwa krajowej sieci telekomunikacyjnej.
- Praktyki, nie mają charakteru standardu, ale ich głównym celem jest ochrona krytycznej infrastruktury sieciowej.
- Uważa się iż wiele dotychczasowych awarii nie miałoby miejsca gdyby wcześniej zaimplementowano najlepsze praktyki.

Standardy umożliwiające certyfikacje

ISO/IEC 15408 (Common Criteria)

- Międzynarodowa norma Common Criteria(wspólne, powszechne kryteria) (ISO/IEC 15408) definiuje kryteria oceny bezpieczeństwa systemów teleinformatycznych. pozwalająca w sposób formalny weryfikować bezpieczeństwo systemów teleinformatycznych.
- Common Criteria udostępnia procedury pozwalające na zdefiniowanie zagrożeń oraz zabezpieczeń, które na te zagrożenia odpowiadają, a następnie przeprowadzenie formalnej weryfikacji ich faktycznego działania w systemie, produkcie.

ISO/IEC 15408 (Common Criteria)

- Certyfikacją według normy Common Criteria zajmują się niezależne, akredytowane laboratoria badawcze na całym świecie.
- Wynikiem procesu certyfikacji jest tzw. "profil ochrony" (PP - *protection profile*), który definiuje zabezpieczenia stosowane przez produkt oraz certyfikat, potwierdzający ich faktyczną skuteczność.

PN-I-07799-2

- Wymagania te są podstawa do wydawania certyfikatów „bezpieczeństwa”, tj. certyfikatów na zgodność z norma PN-I-
- 07799-2:2005. Z reguły certyfikat wydawany jest na 3 lata, a potem koniecznym jest przystąpienie do recertyfikacji w celu przedłużenia ważności certyfikatu.

PN-I-07799-2

- Wymagania te są podstawa do wydawania certyfikatów „bezpieczeństwa”, tj. certyfikatów na zgodność z norma PN-I-07799-2:2005. Z reguły certyfikat wydawany jest na 3 lata, a potem koniecznym jest przystąpienie do recertyfikacji w celu przedłużenia ważności certyfikatu.

ISO/IEC 27000

- Celem opracowania grupy norm ISO 27000 jest zebranie i ujednolicenie dotychczasowych opracowań i standardów poświęconych bezpieczeństwu informacji. W skład tej grupy wchodzą następujące normy:
- ISO/IEC 27001:2005 – wymagania związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.
- ISO/IEC 27002 – ma zastąpić normę ISO/IEC 17799:2005 – wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji.

ISO/IEC 27000

- ISO/IEC 27003 – porady i wskazówki dotyczące implementacji Systemu Zarządzania Bezpieczeństwem Informacji.
- ISO/IEC 27004 – wskaźniki i pomiar dotyczący SZBI.
- ISO/IEC 27005 – wzorzec może stanowić norma BS 7799-3 – szacowania ryzyka w Systemie Zarządzania Bezpieczeństwem Informacji.
- ISO/IEC 27006 – wytyczne do certyfikacji Systemu Zarządzania Bezpieczeństwem Informacji.
- ISO/IEC 2700 – dobre praktyki dla przeprowadzania audytów wewnętrznych i certyfikacyjnych Systemów Zarządzania Bezpieczeństwem Informacji.

ISO/IEC 27000

- ISO/IEC 27011 – norma będzie stanowić rozszerzenie ISO 27001/27002 o dobre praktyki dla przemysłu telekomunikacyjnego. Prace nad tym standardem trwają, jednak nie należy spodziewać się ich ukończenia przed rokiem 2010.
- ISO/IEC 27031 – ICT – standard dotyczyć będzie ciągłości działania. Przewiduje się, że opierać się będzie na standardach SS507 oraz BS 25999.
- ISO/IEC 27032 – jest to propozycja dla opracowania standardu dotyczącego bezpieczeństwa w Internecie.
- ISO/IEC 27033 – jest to propozycja zastąpienia istniejącego standardu ISO/IEC 18028:2006 dotyczącego bezpieczeństwa sieci teleinformatycznych.
- ISO/IEC 27034 – propozycja stworzenia standardu bezpieczeństwa dla aplikacji.
- ISO/IEC 27799 – wersja ISO 27002 dedykowana dla sektora medycznego.

Organizacje i wydawane przez nie certyfikaty

- **ISACA** - już było
- **IIA** (***The Institute of Internal Auditors***) to najstarsza i największa na świecie organizacja audytorów wewnętrznych. Skupia ponad 100.000 osób w ok. 200 oddziałach na świecie.
- W Polsce istnieje jako Stowarzyszenie Audytorów Wewnętrznych IIA Polska i zrzesza ponad 650 osób z całego kraju.
- Certyfikat CIA (*Certified Internal Auditor*), przyznawany dla osób, które zdając egzamin, wykazały się wiedzą, umiejętnościami i kwalifikacjami do wykonywania zawodu audytora wewnętrznego.
- Certyfikat może być rozszerzony o certyfikaty: CFSA (*Certified Financial Services Auditor*), CGAP (*Certified Government Auditing Professional*) oraz CCSA (*Certification In Control Self-Assessment*)

PIKW

- Polski Instytut Kontroli Wewnętrznej powstał w 1998r. Jest to organizacja przygotowująca kadry do profesjonalnej oceny systemów kontroli wewnętrznej i audytu wewnętrznego zgodnie ze standardami i najlepszymi, sprawdzonymi praktykami kontroli wewnętrznej i audytu wewnętrznego Unii Europejskiej.
- PIKW i związani z nim czołowi audytorzy i kontrolerzy są założycielami i członkami Stowarzyszenia Audytorów Wewnętrznych – IIA Polska oraz Stowarzyszenia Biegłych ds. Wykrywania i Zapobiegania Oszustwom i Nadużyciom: ACFE Polska.

Standardy typu „best practice”

K O N I E C