BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 26, 2009

# Normy i standardy z zakresu bezpieczeństwa informacyjnego i teleinformatycznego

**Krzysztof LIDERMAN**

Zakład Systemów Komputerowych, Instytut Teleinformatyki i Automatyki WAT
ul. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: Artykuł zawiera przegląd norm i standardów z zakresu bezpieczeństwa teleinformatycznego nieco mniej znanych niż normy serii ISO/IEC 27000 oraz ISO/IEC 15408.

SŁOWA KLUCZOWE: NIST, CAG, ITIL, COBIT, SSE-CMM.

## 1. Wstęp

Obecnie w dziedzinie szeroko rozumianego bezpieczeństwa teleinformatycznego największą popularność ma dwuczęściowa norma ISO/IEC 27001/2 (w zakresie zarządzania systemem bezpieczeństwa informacji) oraz standard Common Criteria (w zakresie oceny i wytycznych do budowy „bezpiecznych" systemów przetwarzania informacji). Norma ISO/IEC 27001 ma swój polski odpowiednik w normie PN-ISO/IEC-27001:2007 [5], norma ISO/IEC 27002 w normie PN-ISO/IEC-17799:2007 [4], a standard Common Criteria w trzyczęściowej normie ISO/IEC 15408, także z polskim odpowiednikiem dla części 1 i 3 (por. [6], [7]).

Wymienione normy[1] były już opisywane w biuletynie IAiR [1], [2], [3]. Niniejszy artykuł ma na celu przedstawienie norm i standardów nieco mniej popularnych, ale niewątpliwie zasługujących na uwagę tych wszystkich osób, które zajmują się budowaniem, nadzorowaniem i oceną systemów ochrony informacji.

[1] W przypadku normy PN-ISO/IEC 27001 jej starszy odpowiednik to PN-I-07799-2:2005.

## 2. SSE-CMM® – System Security Engineering Capability Maturity Model (v.3.0)

Projekt SSE-CMM jest rozwijany od 1993 roku jako uszczegółowiony wariant opracowanego w Carnegie Mellon University modelu dojrzałości organizacyjnej CMM®[2]. Głównymi sponsorami projektu są:

- National Security Agency (USA),
- Office of the Secretary of Defense (USA),
- Communications Security Establishment (Kanada).

Celem projektu, w którego rozwój jest zaangażowanych ponad 50 organizacji z różnych krajów, jest **rozwijanie inżynierii bezpieczeństwa w kierunku dobrze zdefiniowanej, dojrzałej i mierzalnej dziedziny działalności inżynierskiej**. Do rozwijania i promocji tego projektu została powołana organizacja *International Systems Security Engineering Association* (ISSEA – www.issea.org), która we współpracy z ISO doprowadziła do wydania normy: ISO/IEC 21827:2008 *Information technology – Security techniques –Systems Security Engineering – Capability Maturity Model® (SSE-CMM®)*.

Opracowany w ramach projektu model SSE-CMM może być zastosowany do:

1. Udoskonalenia procesów z zakresu bezpieczeństwa (*process improvement*).
2. Oceny „dojrzałości" w zakresie bezpieczeństwa (*capability evaluation*).
3. Budowy zaufania (*assurance*), że produkt (system, usługa) został wykonany przy zachowaniu wymaganych środków z zakresu bezpieczeństwa.

Na model architektury SSE-CMM składa się:

1. Zestaw tzw. *ogólnych praktyk* (oznaczanych w opisach jako GPx.y.z), podzielonych pomiędzy pięć poziomów doskonałości, opisujących działania z zakresu zarządzania, uzupełniających najlepsze praktyki z dziedziny bezpieczeństwa.
2. 129 tzw. *najlepszych praktyk* (oznaczanych w opisach jako BPx.y) z 22 obszarów, podzielonych następująco:
   - 61 praktyk (opracowanych na podstawie różnych źródeł) w 11 obszarach *Security Engineering Process Areas*;

[2] CMM® jest pięciostopniowym „wzorcem doskonałości", który proces może osiągać poprzez coraz precyzyjniejsze definiowanie, implementowanie i udoskonalanie.

- 68 praktyk (opracowanych na podstawie Systems Engineering and Software CMM) w 11 obszarach *Project and Organizational Process Areas*.

3. Pięć poziomów doskonałości:

   Poziom 1 – nieformalny (*performed informally*).

   Poziom 2 – planowy i monitorowany (*planned and tracked*).

   Poziom 3 – dobrze zdefiniowany (*well defined*).

   Poziom 4 – mierzalny (*quantitatively controlled*).

   Poziom 5 – udoskonalany (*continuously improving*).

Stosowane w opisie praktyk określenie:

- *defined process* – oznacza, co inżynierowie od bezpieczeństwa zamierzają w tej dziedzinie robić;
- *performed process* – oznacza, co inżynierowie od bezpieczeństwa aktualnie w tej dziedzinie robią;
- *process capability* – oznacza mierzalne rezultaty realizacji określonego procesu.

**Przykład_1:**

Format opisu najlepszych praktyk PAxx (słowa kluczowe *kursywą* jak w oryginale).

**PA01** – ***Process Area Title*** nazwa obszaru (w formie imiesłowowej).

| | |
|---|---|
| *Summary Description* | krótka charakterystyka tego obszaru procesowego; |
| *Goals* | lista oczekiwanych rezultatów implementacji tego obszaru procesowego; |
| *Base Practices List* | specyfikacja najlepszych praktyk z tego obszaru procesowego; |
| *Process Area Notes* | uwagi dodatkowe nt. tego procesu. |

**BP.01.01** – ***Base Practice Title*** nazwa praktyki (w formie imiesłowowej).

| | |
|---|---|
| *Descriptive Name* | pełna nazwa praktyki; |
| *Description* | opis praktyki; |
| *Example Work Products* | lista przykładowych, oczekiwanych produktów wyjściowych zastosowania praktyki; |
| *Notes* | uwagi dodatkowe nt. tej praktyki. |

**BP.01.02** …

…

W podobny sposób są opisane praktyki ogólne GPx.y.z pogrupowane w zbiory cech (*common features*) charakteryzujące podstawowe właściwości poziomów dojrzałości organizacyjnej.

**Tab. 1. Związki pomiędzy elementami modelu SSE-CMM**

| | | PA01 – Administer Security Controls | PA02 – Assess Impact | PA03 – Assess Security Risk | PA04 – Assess Threat | PA05 – Assess Vulnerability | PA06 – Build Assurance Argument | PA07 – Coordinate Security | PA08 – Monitor Security Posture | PA09 – Provide Security Input | PA10 – Specify Security Needs | PA11 – Verify and Validate Security | PA12 – Ensure Quality | PA13 – Manage Configuration | PA14 – Manage Project Risk | PA15 – Monitor and Control Techn. Effort | PA16 – Plan Technical Effort | PA17 – Define Org. Systems Eng. Process | PA18 – Improve Org. Systems Eng. Process | PA19 – Manage Product Line Evolution | PA20 – Manage Systems Eng. Support Env. | PA21 – Provide Ongoing Skills and Knidge | PA22 – Coordinate with Suppliers |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| POZIOM 5 | 5.2. Improving Proc. Effective-ness | | | | | | | | | | | | | | | | | | | | | | |
| | 5.1. Improving Org. Capability | | | | | | | | | | | | | | | | | | | | | | |
| POZIOM 4 | 4.2. Objectively Managing Perf. | | | | | | | | | | | | | | | | | | | | | | |
| | 4.1. Establish Meas. Quality Goals | | | | | | | | | | | | | | | | | | | | | | |
| POZIOM 3 | 3.3. Coordinate Practices | | | | | | | | | | | | | | | | | | | | | | |
| | 3.2 Perform the Defined Process | | | | | | | | | | | | | | | | | | | | | | |
| | 3.1 Defining a Standard Process | | | | | | | | | | | | | | | | | | | | | | |
| POZIOM 2 | 2.4 Tracking Performance | | | | | | | | | | | | | | | | | | | | | | |
| | 2.3 Verifying Performance | | | | | | | | | | | | | | | | | | | | | | |
| | 2.2 Disciplined Performance | | | | | | | | | | | | | | | | | | | | | | |
| | 2.1 Planned Performance | | | | | | | | | | | | | | | | | | | | | | |
| POZIOM 1 | 1.1 Base Practices Are Performed | | | | | | | | | | | | | | | | | | | | | | |
| **Common Features** | | | | | | | | | | | | | | | | | | | | | | | |
| **Process Areas** | | | | | | | | | | | | | | | | | | | | | | | |
| | | **Security Engineering Process Areas** | | | | | | | | | | | **Project and Organizational Process Areas** | | | | | | | | | | |

Tabela 1 pokazuje związki pomiędzy poszczególnymi elementami modelu SSE-CMM. Warto zauważyć, że przy takiej prezentacji łatwo pokazać dojrzałość organizacyjną firmy w zakresie poszczególnych procesów (przykładowe, zacieniowane komórki w części głównej tabeli).

## 3. Publikacje specjalne NIST serii 800

*National Institute of Standards and Technology* jest organizacją opracowującą standardy i zalecenia techniczne dla administracji rządowej USA. Szczególnie cenne dla osób zajmujących się ochroną informacji są publikacje specjalne (SP – *Special Publication*) dostępne w formacie pdf pod adresem http://csrc.nist.gov/publications/PubsSPs.html. Krótka lista tych publikacji jest następująca:

1. **SP-800-39:** Managing Risk from Information Systems. *An Organizational Perspective*.
2. **SP-800-48:** Wireless Network Security for IEEE 802.11a/b/g and Bluetooth.
3. **SP-800-50:** Building an Information Technology Security Awareness and Training Program.
4. **SP-800-53:** Recommended Security Controls for Federal Information System.
5. **SP-800-53A**: Guide for Assessing the Security Controls in Federal Information Systems. *Building Effective Security Assessment Plans*.
6. **SP-800-60:** Volume **I**: Guide for Mapping Types of Information and Information Systems to Security Categories. Volume **II**: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.
7. **SP-800-61:** Computer Security Incident Handling Guide.
8. **SP-800-64:** Security Considerations in the Information System Development Life Cycle.
9. **SP-800-82:** Guide to Industrial Control Systems (ICS) Security.
10. **SP-800-86:** Guide to Computer and Network Data Analysis: *Applying Forensic Techniques to Incident Response*.
11. **SP-800-92:** Guide to Computer Security Log Management.
12. **SP-800-95:** Guide to Secure Web Services.
13. **SP-800-100:** Information Security Handbook: *A Guide for Managers*.
14. **SP-800-115:** Technical Guide to Information Security Testing.

Osoby budujące systemy zabezpieczeń powinny przede wszystkim zapoznać się z zaleceniami zawartymi w SP-800-53. Natomiast osobom, które chcą sobie wyrobić pogląd na zakres przedsięwzięć związanych z zapewnianiem szeroko rozumianego bezpieczeństwa teleinformatycznego (i jednocześnie zakresem dostępnych publikacji NIST), a nie mają czasu na studiowanie wszystkich dokumentów serii SP-800, poleca się publikację SP800-100. Na jej

178 stronach zawarty jest przegląd takich przedsięwzięć wraz z odsyłaczami do innych publikacji tej serii, w których poszczególne zagadnienia są szczegółowo opisane.

## 4. Standardy Brytyjskiego Instytutu Standaryzacji

Oznaczone symbolem BS standardy Brytyjskiego Instytutu Standaryzacji (BSI – *British Standard Institute*) z zakresu zarządzania bezpieczeństwem informacji cieszą się dużym uznaniem na całym świecie, czego przejawem jest m.in. przyjęcie ich za podstawę szeregu norm z zakresu bezpieczeństwa teleinformatycznego i ochrony informacji, wydawanych przez *International Standard Organisation* w serii oznaczonej jako ISO/IEC 270xx. W niniejszym opracowaniu zostanie krótko zaprezentowany jeden ze standardów, który ma szansę na takie wydanie.

Standard BS 25999-1 [9] został opublikowany w 2006 roku. Zawiera wyjaśnienie terminologii z zakresu zarządzania ciągłością działania (BCM – *Business Continuity Management*), opis podstawowych zasad (tzw. dobrych praktyk, ang. *good practice*) takiego zarządzania oraz identyfikuje podstawowe procesy z tym związane. Od strony praktycznej, BS 25999-1 stanowi zbiór objaśnień do wymagań zawartych w części drugiej.

Standard BS 25999-2 [10] został opublikowany w 2007 roku. Określa wymagania dla systemów zarządzania ciągłością działania – ustanowienia, wdrożenia, eksploatacji, przeglądu, testowania, utrzymania i doskonalenia dokumentowanego systemu zarządzania ciągłością (*Business Continuity Management System* – BCMS) w kontekście kompleksowego zarządzania ryzykiem działalności. W szczególności, pokazuje związki z lansowanym przez BSI tzw. *cyklem Deminga* (PDCA – Plan, Do, Check, Act) stanowiącym model dla systemu zarządzania bezpieczeństwem informacji (por. norma PN-ISO/IEC 27001).

Wymagania określone w normie są zaprojektowane tak, aby pasowały do każdej organizacji (lub jej części) niezależnie od rodzaju i wielkości działalności. Zakres wdrożenia wymagań uzależniony jest od rodzaju otoczenia, w jakim organizacja funkcjonuje, oraz złożoności samej organizacji. Z tego względu projekt i sposób wdrożenia BCMS będzie uzależniony od wymagań prawnych, klientów oraz wymagań wynikających ze sposobu prowadzania działalności, rodzaju oferowanych produktów i usług, procesów funkcjonujących w organizacji, jej wielkości i struktury. Celem standardu nie jest ujednolicenie struktur systemów zarządzania, ale wdrożenie takiego systemu, który będzie odpowiadał potrzebom biznesu i zaspokajał oczekiwania udziałowców.

BS 25999-2 może być wykorzystywany do wewnętrznej, a także zewnętrznej oceny systemów, w tym przez jednostki certyfikujące, do oceny zdolności organizacji do spełnienia jej potrzeb w zakresie ciągłości działania, a także realizacji wymagań: klientów oraz przepisów prawa.

## 5. COBIT®

ISACA (*Information Systems Audit and Control Association*) to Stowarzyszenie do Spraw Audytu i Kontroli Systemów Informatycznych[3]. Celem Stowarzyszenia jest działalność edukacyjna służąca podnoszeniu oraz rozwijaniu wiedzy i umiejętności jego członków w zakresie prowadzenia audytu oraz świadczenia usług doradczych w dziedzinie audytu i kontroli systemów informatycznych. ISACA opracowuje standardy, prowadzi szkolenia i certyfikacje. Najbardziej znanymi działaniami ISACA są:

1) program certyfikacji osób:
   - CISA (*Certified Information System Auditor*),
   - CISM (*Certified Information System Manager*);
2) opracowanie i opublikowanie w 1996 roku standardu COBIT® (*Control Objectives for Information and Related Technology*).

Podstawowe części wymienionego standardu to:

- Executive Summary,
- Framework,
- Control Objectives,
- Audit Guidelines,
- Implementation Tool Set.

Zasadniczą częścią tego zestawu są *Control Objectives*, które zawierają 214[4] szczegółowych wymagań przypisanych do 34 procesów realizowanych w systemach teleinformatycznych. Przez członków ISACA, COBIT jest nazywany *schematem ładu informatycznego*, który umożliwia kierownictwu firmy opracowanie dobrych praktyk nadzoru i kontroli działów informatycznych (IT) w firmie. W COBIT 4.1 opisano:

- 4 domeny informatyczne:
  - PO – Planowanie i Organizacja
  - AI – Nabywanie i Wdrażanie

[3] Strona internetowa Polskiego Oddziału ISACA dostępna pod: www.isaca.org.pl.
[4] W wersji 4.1, dostępnej jako PDF pod www.isaca.org – stan na początek roku 2009.

  - DS – Dostarczanie i Obsługa
  - ME – Monitorowanie i Ocena.
- 34 procesy IT.
- 31 ogólne cele kontrolne.
- 214 szczegółowych celów kontrolnych przypisanych poszczególnym procesom.
- 7 kryteriów jakości przetwarzania informacji: *efektywność, wydajność, poufność, integralność, dostępność, zgodność, rzetelność*.
- 4 rodzaje zasobów: *aplikacje, informacje, infrastruktura, ludzie*.
- Mechanizmy kontrolne w aplikacji (AC), zdefiniowane jako zautomatyzowane mechanizmy kontrolne zakodowane w aplikacji biznesowej.
- Macierze odpowiedzialności (RCAI), zawierające wytyczne odnośnie ról i odpowiedzialności na poszczególnych stanowiskach, czyli kto będzie *rozliczany* (A), *odpowiedzialny* (R), *konsultowany* (C), *informowany* (I).
- Wskaźniki wyznaczone dla procesów IT, pokazujące jak te procesy spełniają cele biznesowe IT. Obejmują one:
  - kluczowe wskaźniki *wydajności,*
  - kluczowe wskaźniki *celu procesu,*
  - kluczowe wskaźniki *celu IT*.
- Poziomy dojrzałości procesów (CMM): *brak* (0), *początkowy* (1), *powtarzalny* (2), *zdefiniowany* (3), *zarządzany* (4), *zoptymalizowany* (5).

Tabela 2 pokazuje w syntetyczny sposób lansowaną przez ISACA ideę audytu informatycznego. Poszczególne wiersze zawierają procesy biznesowe organizacji związane z wykorzystaniem informatyki, kryteria oceny tych procesów (1–7) oraz zasoby których dotyczą (I–V). Dla każdego procesu w COBIT są zdefiniowane tzw. punkty kontrolne (w sumie jest ich 302 w wersji 2 standardu i 318 w wersji 3), dla których osoba przeprowadzająca ocenę musi znaleźć uzasadnione potwierdzenie ich spełnienia lub nie spełnienia w ramach ocenianej organizacji. Na przykład, dla procesu DS12 „Zarządzanie urządzeniami", punkty kontrolne dotyczą:

- DS12.1: bezpieczeństwa fizycznego,
- DS12.2: utrudnienia osobom obcym identyfikacji rozmieszczenia sprzętu komputerowego,
- DS12.3: nadzoru nad osobami obcymi przebywającymi na terenie organizacji,
- DS12.4: BHP,
- DS12.5: przeciwdziałania skutkom zagrożeń środowiskowych (upał, wilgoć, ogień itd.),
- DS12.6: zasilania awaryjnego.

**Tab. 2. Audyt informatyczny według COBIT**

| | | **Kryteria** | | | | | | | **Zasoby informatyczne** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **PROCES** | **NAZWA** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | I | II | III | IV | V |
| **Planowanie i organizowanie** | | | | | | | | | | | | | |
| PO1 | Definiowanie planu strategicznego IT | P | S | | | | | | X | X | X | X | X |
| PO2 | Definiowanie architektury IT | P | S | S | S | | | | | X | | | X |
| PO3 | Determinowanie kierunku technologicznego | P | S | | | | | | | | X | X | |
| PO4 | Definiowanie organizacji i relacji IT | P | S | | | | | | X | | | | |
| PO5 | Zarządzanie inwestycjami IT | P | P | | | | | S | X | X | X | X | |
| PO6 | Przedstawienie celów i kierunków rozwoju formułowanych przez kierownictwo | P | | | | | S | | X | | | | |
| PO7 | Zarządzanie zasobami ludzkimi | P | P | | | | | | X | | | | |
| PO8 | Zapewnianie zgodności z wymogami otoczenia | P | | | | | P | S | X | X | | | X |
| PO9 | Szacowanie ryzyka | S | S | P | P | P | S | S | X | X | X | X | X |
| PO10 | Zarządzanie projektami | P | P | | | | | | X | X | X | X | |
| PO11 | Zarządzanie jakością | P | P | | P | | | S | X | X | | | |
| **Nabywanie i wdrażanie** | | | | | | | | | | | | | |
| AI1 | Identyfikacja rozwiązań | P | S | | | | | | | X | X | X | |
| AI2 | Nabywanie i utrzymywanie oprogramowania aplikacyjnego | P | P | | S | | S | S | | X | | | |
| AI3 | Nabywanie i utrzymywanie architektury technologicznej | P | P | | S | | | | | | X | | |
| AI4 | Rozwijanie i utrzymywanie procedur IT | P | P | | S | | S | S | X | X | X | X | |
| AI5 | Instalowanie i akredytowanie systemów | P | | | S | S | | | X | X | X | X | X |
| AI6 | Zarządzanie zmianami | P | P | | P | P | | S | X | X | X | X | X |
| **Dostarczanie i wspieranie** | | | | | | | | | | | | | |
| DS1 | Definiowanie poziomów serwisowych | P | P | S | S | S | S | S | X | X | X | X | X |
| DS2 | Zarządzanie obcym serwisem | P | P | S | S | S | S | S | X | X | X | X | X |
| DS3 | Zarządzanie efektywnością i wydajnością | P | P | | | S | | | | X | X | X | |
| DS4 | Zapewnianie ciągłości serwisu | P | S | | | P | | | X | X | X | X | X |
| DS5 | Zapewnianie bezpieczeństwa systemów | | | P | P | S | S | S | X | X | X | X | X |
| DS6 | Identyfikowanie i przypisywanie kosztów | | P | | | | | P | X | X | X | X | X |
| DS7 | Edukowanie i szkolenia użytkowników | P | S | | | | | | X | | | | |
| DS8 | Asystowanie i pomaganie klientom IT | P | | | | | | | X | X | | | |
| DS9 | Zarządzanie konfiguracją | P | | | | S | | S | | X | X | X | |
| DS10 | Zarządzanie problemami i incydentami | P | P | | | S | | | X | X | X | X | X |
| DS11 | Zarządzanie danymi | | | | P | | | P | | | | | X |
| DS12 | Zarządzanie urządzeniami | | | | P | P | | | | | | X | |
| DS13 | Zarządzanie operacjami | P | P | | S | S | | | X | X | | X | X |
| **Monitorowanie** | | | | | | | | | | | | | |
| M1 | Monitorowanie procesów | P | S | S | S | S | S | S | X | X | X | X | X |
| M2 | Ocena odpowiedniości kontroli wewnętrznej | P | P | S | S | S | S | S | X | X | X | X | X |
| M3 | Uzyskiwanie niezależnej opinii | P | P | S | S | S | S | S | X | X | X | X | X |
| M4 | Zapewnienie niezależnego audytu | P | P | S | S | S | S | S | X | X | X | X | X |

**Oznaczenia:**

P – znaczenie pierwszorzędne dla oceny procesu wykorzystania i przetwarzania informacji;

S – znaczenie drugorzędne dla oceny procesu wykorzystania i przetwarzania informacji;

Kryteria oceny procesu wykorzystania i przetwarzania informacji: 1 – skuteczność, 2 – wydajność, 3 – poufność, 4 – integralność, 5 – dostępność, 6 – zgodność, 7 – rzetelność;

Zasoby informatyczne: I – ludzie, II – aplikacje, III – technologie, IV – urządzenia, V – dane.

## 6. ITIL – IT Infrastructure Library

Podstawowe etapy rozwoju, wymienionego w tytule rozdziału standardu, są następujące:

1) ITIL v.1 – koniec lat 80-tych; zestaw 40 publikacji zbierających *najlepsze praktyki* w zakresie zarządzania usługami IT, opracowany przez brytyjską rządową agendę *Office of Government Commerce*.
2) ITIL v.2 – lata 1999-2002; aktualizacja i konsolidacja wiedzy z zakresu *Service Management* w formie 7 podręczników (opracowane przez OGC i niezależną organizację *IT Service Management Forum*).
3) ITIL v.3 – czerwiec 2007; nowa filozofia – ukierunkowanie na cykl życia usługi zamiast na obszary – opisana w 5 podręcznikach i tzw. publikacjach uzupełniających (w tym COBIT oraz ISO/IEC 27001).

Szkielet ITIL określa procesy zarządzania, ich wejście/wyjście oraz powiązania i zakres odpowiedzialności (por. rys. 1). Cele procesów, określane jako trzy podstawowe punkty „filozofii" ITIL, to:

1. Dostarczanie usług IT (nie systemów!) zorientowanych biznesowo.
2. Długoterminowa redukcja kosztów.
3. Stała kontrola mająca na celu poprawę jakości usług.

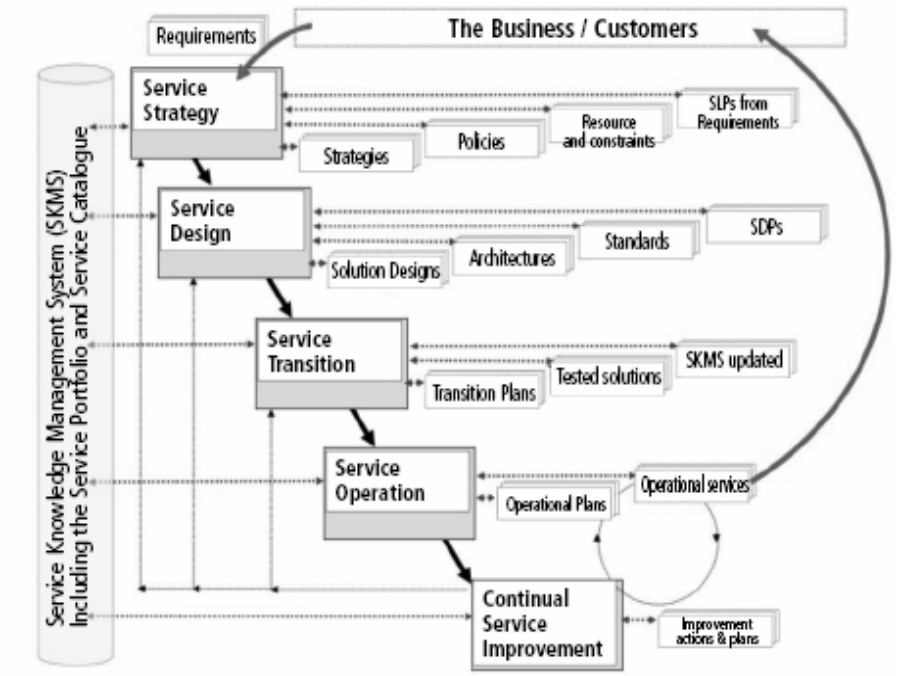
„Najlepsze praktyki" z zakresu zarządzania, zapisane w ITIL, z powodzeniem mogą być stosowane jako wykładnia operacyjna dla zapisów normatywnych dotyczących np. systemów zarządzania bezpieczeństwem informacji (SZBI, norma PN-ISO/IEC 27001).

**Przykład_2:**

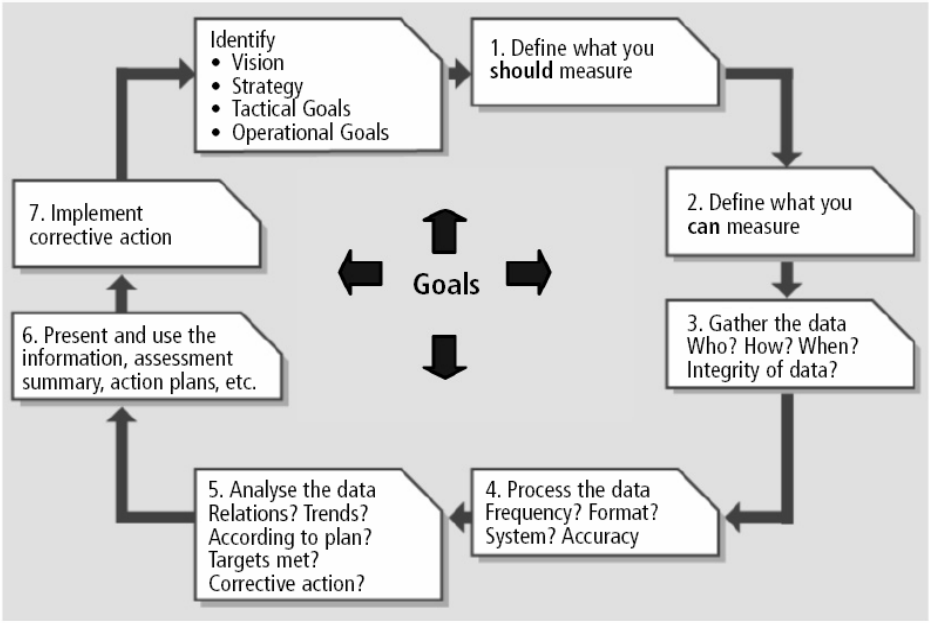
Zostało wykonane „mapowanie" ITIL v.3 na COBIT® 4.1 (szczegóły – por. www.isaca.org/cobitmapping).

**Przykład_3:**

Dla etapu „kontroluj" cyklu PDCA można stosować zapisaną w ITIL 7-mio punktową metodę polepszania wykonania zadania (rys. 2).




**Rys. 1. Podstawowe powiązania oraz wejścia i wyjścia etapów cyklu życia usługi (za [11])**




**Rys. 2. Procedura doskonalenia wykonania zadania (za [11])**

## 7. Nowa inicjatywa nowej administracji USA – Consensus Audit Guideline

W USA, 27 lutego 2009, w ramach ostatnio modnego i marketingowo „nośnego" hasła „cyberdefense", opublikowano *Consensus Audit Guidelines*[5] (data wydania: 23.02.2009). W dokumencie, mocno promowanym m.in. przez instytut SANS, można przeczytać:

▪ *This consensus document is designed to begin the process of establishing that* ***prioritized baseline of information security measures and controls****. The consensus effort that has produced this document has identified twenty specific security controls that are viewed as essential for blocking known high priority attacks.* ▪

W CAG wyspecyfikowano 20 przedsięwzięć niezbędnych (zdaniem autorów opracowania) do szybkiego zabezpieczenia systemu i sieci komputerowej przed „cyberatakami". Każdy z 20 punktów (przedsięwzięć), zatytułowany *Critical Control xx***,** składa się z trzech części:

– *How do attackers export the lack of this control?*; opisującej sposób wykorzystania niezabezpieczonej podatności.
– *How can this control be implemented, automated, and its effectiveness measured?*; podającej, w postaci czterech grup zaleceń, sposoby minimalizowania wyspecyfikowanej podatności.
– *Procedures and tools for implementing this control*; zawierajacej wskazówki na temat możliwości wspomagania procesu zabezpieczania narzędziami programowymi i przedsięwzięciami organizacyjnymi.

Warto zwrócić uwagę, że twórcy opisywanego dokumentu obawiają się (i chcą się chronić) **tylko przed „cyberatakami"** (nie obawiają się zatem działania sił wyższych, awarii oraz błędów ludzkich ).

Dwadzieścia podstawowych przedsięwzięć zabezpieczających przed „cyberatakami" zdefiniowanych w *Consensus Audit Guideline Controls* to:

1. *Inventory of Authorized and Unauthorized Hardware* (inwentaryzacja autoryzowanego i nieautoryzowanego sprzętu).
2. *Inventory of Authorized and Unauthorized Software* (inwentaryzacja autoryzowanego i nieautoryzowanego oprogramowania).

[5] Do pobrania: http://www.csis.org/media/csis/pubs/090223_cag_1_0_draft4.1.pdf .
Dostępne także pod: http://www.sans.org/cag/.

3. *Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers* (utwardzająca konfiguracja sprzętu i oprogramowania na laptopach, stacjach roboczych i serwerach).
4. *Secure Configurations of Network Devices such as Firewalls and Routers* (utwardzająca konfiguracja urządzeń sieciowych takich jak zapory sieciowe i rutery).
5. *Boundary Defense* (ochrona brzegowa).
6. *Maintenance and Analysis of Complete Security Audit Logs* (utrzymywanie i analiza dzienników bezpieczeństwa).
7. *Application Software Security* (bezpieczeństwo aplikacji).
8. *Controlled Use of Administrative Privileges* (kontrola używania uprawnień administracyjnych).
9. *Controlled Access Based on Need to Know* (kontrola dostępu na podstawie wiedzy koniecznej).
10. *Continuous Vulnerability Testing and Remediation* (ciągłe testowanie podatności i ich minimalizowanie).
11. *Dormant Account Monitoring and Control* (monitorowanie i kontrola nieaktywnych kont).
12. *Anti-Malware Defenses* (ochrona przed programami i kodami złośliwymi).
13. *Limitation and Control of Ports, Protocols and Services* (ograniczanie i kontrola portów, protokołów oraz usług).
14. *Wireless Device Control* (kontrola urządzeń bezprzewodowych).
15. *Data Leakage Protection* (przeciwdziałanie wyciekowi danych).

Dodatkowe przedsięwzięcia, nie mające bezpośredniego zautomatyzowanego wsparcia, to:

16. *Secure Network Engineering* (bezpieczna architektura sieciowa).
17. *Red Team Exercises* (ćwiczenia zespołów typu Red Team).
18. *Incident Response Capability* (reagowanie na incydenty).
19. *Data Recovery Capability* (odtwarzanie danych po katastrofie).
20. *Security Skills Assessment and Training to Fill Gaps* (szkolenia z zakresu bezpieczeństwa teleinformatycznego).

Na każde z przedsięwzięć głównych składa się szereg przedsięwzięć o mniejszym zakresie, pogrupowanych w części „How can this control be implemented, automated, and its effectiveness measured?" w następujące zbiory:

- *Quick Wins* (QW): zawiera wskazówki, gdzie/jak można szybko i tanio starać się zminimalizować podatności, poprawiając tym samym ogólny stan ochrony organizacji przed „cyberatakami".
- *Improved Visibility and Attribution* (Vis/Attrib.): zawiera wskazówki, jak uwidocznić/szukać potencjalnych celów ataków poprzez monitorowanie i strukturyzowanie (przypisywanie atrybutów do procesów i zasobów) organizacji.
- *Hardened Configuration and Improved Information Security Hygiene* (Config/Hygiene): zawiera wskazówki nt. utwardzania programów, urządzeń i systemów.
- *Advanced* (Advanced): zawiera zalecenia co jeszcze, w przyszłości, może zrobić organizacja, żeby ochronić się przed „cyberatakami".

## 8. Podsumowanie

Na zakończenie niniejszego krótkiego przeglądu norm i standardów, warto zwrócić uwagę na sposób ich udostępniania. Common Criteria[6], COBIT, SSE-CMM, CAG i standardy NIST są dostępne w Internecie, za darmo. To pozytywnie odróżnia je od norm i standardów wydawanych przez takie organizacje jak ISO czy Polski Komitet Normalizacyjny – ich normy trzeba kupić.

## Literatura:

[1] LIDERMAN K., *Międzynarodowe kryteria oceny bezpieczeństwa informacji w systemach informatycznych*, Biuletyn IAiR, Nr 11, str. 43-57, WAT, Warszawa, 2000.

[2] LIDERMAN K., *Standardy w ocenie bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, Nr 17, str. 97-119, WAT, Warszawa, 2002.

[3] LIDERMAN K., Przegląd normy PN-I-07799-2:2005, *Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania*, Biuletyn IAiR, Nr 22, str. 71-92, WAT, Warszawa, 2005.

[4] PN-ISO/IEC-17799:2007: *Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji*.

[6] Dostępne pod http://www.commoncriteriaportal.org/thecc.html.

[5] PN-ISO/IEC 27001:2007: *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*.

[6] PN-ISO/IEC 15408-1:2002: *Technika informatyczna - Techniki zabezpieczeń - Kryteria oceny zabezpieczeń informatycznych - Część 1: Wprowadzenie i model ogólny*.

[7] PN-ISO/IEC 15408-3:2002: *Technika informatyczna - Techniki zabezpieczeń - Kryteria oceny zabezpieczeń informatycznych - Część 3: Wymagania uzasadnienia zaufania do zabezpieczeń*.

[8] PN-IEC 62198:2005: *Zarządzanie ryzykiem przedsięwzięcia - Wytyczne stosowania.*

[9] BS 25999-1: 2006: *Business continuity management. Code of practice*.

[10] BS 25999-2: 2007: *Specification for business continuity management*.

[11] CARTLIDGE A., LILLYCROP M. (eds.), *An Introductory Overview of ITIL® V3 Version 1.0,* Published by: The UK Chapter of the it SMF, 2007.

## Information security and computer safety norms and standards

ABSTRACT: This paper contains information security and computer safety norms and standards review, a little less known than ISO/IEC 27000 and ISO/IEC 15408.

KEY WORDS: NIST, CAG, ITIL, COBIT, SSE-CMM.

*Praca wpłynęła do redakcji: 20.06.2009*