Dobre praktyki zarządzania bezpieczeństwem informacji. Najnowsze standardy ISMS serii ISO/IEC 27000

Jacek ŁUCZAK

Dane i informacje zaliczane są do zasobów o charakterze krytycznym dla prowadzonej działalności, stanowią lub determinują wartość dodaną w aktywności każdej organizacji i dlatego wymagają szczególnej troski – właściwego zarządzania i ochrony.

Bezpieczeństwo informacji w ujęciu systemowym spotyka się z coraz większym zainteresowaniem wielu organizacji. Nie dowodzi tego – lawinowy wzrost liczby certyfikatów, ale świadczą o tym na przykład częste modyfikacje standardów stanowiących podstawę systemów zarządzania w tym zakresie. Na pewno nigdy certyfikaty ISMS nie będą tak popularne jak dotyczące zarządzania jakością, jednak tłumaczy to zdecydowanie specyfika materii jakiej dotyczą. Nie znaczy to jednak, że nie wzrasta świadomość przedsiębiorców co do wagi aktywów informacyjnych dla prowadzonej przez nich działalności, co do rozumienia pojęcia bezpieczeństwa informacji i konieczności systemowego jego ochrony. Często zatem organizacje podejmują zadanie – podniesienie poziomu bezpieczeństwa informacji, jednak przynajmniej na razie niewiele z nich stawia także sobie cel – uzyskanie certyfikatu. Ale dla pierwszego i drugiego podejścia istotne są tzw. dobre praktyki zarządzania bezpieczeństwem informacji, które przybrały postać najnowszych międzynarodowych standardów ISO/ IEC 27001:2005[1] oraz ISO/ IEC 17799:2005[2]. Częstotliwość modyfikacji norm w tym zakresie jest dobrym argumentem potwierdzającym podnoszenie świadomość konieczności ochrony informacji.

Incydenty związane z naruszeniami bezpieczeństwa informacji niejednokrotnie powodują straty finansowe oraz innego rodzaju straty związane z prowadzoną działalnością gospodarczą. Dla niektórych firm okazują się one być kresem ich działalności. Z tych właśnie powodów, niezwykle istotne okazuje się zbudowanie własnej polityki bezpieczeństwa informacji. Jak wskazują eksperci najlepiej oprzeć się w tym zakresie o dobre praktyki benchmarkingowe. Są one zbiorem zagadnień bardzo ogólnie zdefiniowanym – niezwykle dynamicznym, jako że stanowią odpowiedź na bardzo zmienne warunki gospodarcze (różnorodność zagrożeń, prawdopodobieństw ich zajścia i zmienne podatności rozwiązań wobec zmiennych czynników otoczenia). Na pewno zatem na ochronę danych nie można patrzeć przez pryzmat jednostkowych rozwiązań, ale zdecydowanie w ujęciu systemu zarządzania opartego o oszacowane ryzyka. Podstawę taką dają najnowsze standardy: ISO/ IEC 27001:2005 oraz ISO/ IEC 17799:2005. Pierwszy stanowi o wymaganiach koniecznych do spełnienia dla potrzeb certyfikacji systemu, drugi ma charakter przewodnika. Stanowią one kolejne, najnowsze przybliżenie do tych zagadnień i poprzez ich umiędzynarodowienie wskazują na upowszechnianie się problematyki. Standard ISO/ IEC 27001:2005 nabiera szczególnego znaczenia bowiem zastępuje dotychczas najpowszechniejszą normę stanowiącą podstawę ISMS – BS 7799-2. Natomiast ISO/ IEC 17799:2005 daje szerszą perspektywę widzenia bezpieczeństwa informacji, dostarczając ważnego zbioru dobrych praktyk, których rozważanie stanowi istotę utrzymania i doskonalenia ISMS[3]. Pojawienie się międzynarodowej podstawy certyfikacji systemów zarządzania bezpieczeństwem informacji jest godnym odnotowania przełomem – umiędzynarodowienia wcześniejszych brytyjskich wymagań, co najpewniej zwiastuje większe zainteresowanie organizacji tym tematem.

[1] ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements

[2] ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management

[3] ISMS – Information Security Management System (System zarządzania bezpieczeństwem informacji)

Jacek ŁUCZAK

Wg Teda Humphreys`a[4], opublikowanie ISO/IEC 27001:2005 to bardzo wyczekiwane wydarzenie i bardzo pożądany standard w zakresie bezpieczeństwa informacji. Zdaniem organizatora grupy roboczej odpowiedzialnej w ramach ISO za zarządzanie rozwinięciem standardu, jest to zbiór dobrych praktyk zarządzania bezpieczeństwem – bardzo odpowiedni na chwilę obecną.

Istota zasad zarządzania bezpieczeństwem informacji

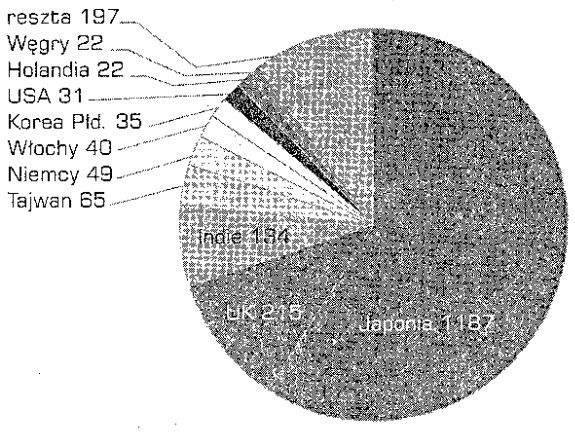
Obserwacja rynkowa dowodzi, że wiele organizacji uświadamiając sobie znaczenie informacji, i potrzebie jej ochrony będzie poszukiwało określonych w tym względzie wytycznych. Dla nich celem jest zapewnienie odpowiedniego poziomu bezpieczeństwa organizacji poprzez właściwą ochronę danych i informacji. Dla niektórych celem będzie także uzyskanie certyfikatu zgodności, dla wielu opracowanie i wdrożenie skutecznej polityki bezpieczeństwa. Obydwa zatem standardy są godne uwagi.

Tab. 1. Liczba akredytowanych certyfikatów ISMS (BS 7799-2) na świecie (stan na grudzień 2005 r.).

Japonia	1187	Czechy	6	Tajlandia	1
UK	215	Brazylia	5	Bahraj	1
Indie	134	Polska	5	Chile	1
Tajwan	65	Hiszpania	5	Kolumbia	1
Niemcy	49	Chorwacja	4	Egipt	1
Włochy	40	Grecja	4	Francja	1
Korea Płd.	35	Islandia	4	Liban	1
USA	31	Arabia Saud.	4	Litwa	1
Węgry	22	Argentyna	3	Luksemburg	1
Holandia	22	Kuwejt	3	Makau	1
Chiny	19	Meksyk	3	Macedonia	1
Hongkong	18	UAE	3	Moroko	1
Australia	17	Belgia	2	Nowa Zelandia	1
Finlandia	15	Kanada	2	Katar	1
Irlandia	11	Dania	2	Rumunia	1
Norwegia	11	Wyspa Man	2	Rosja	1
Singapur	11	Malezja	2	Słowenia	1
Szwajcaria	8	Filipiny	2	Turcja	1
Austria	1	Słowacja	2	SUMA	2001
Szwecja	7	RPA	2		

Źródło: www.xisec.com

ISO/IEC 27001:2005 może być zastosowany przez każdego typu organizację, niezależnie od wielkości, branży czy formy działalności. Praktyka dowodzi że wcześniejsze standardy znajdowały zastosowanie w wielu branżach i nie można mówić o dominujących w tym zakresie. Certyfikaty ISMS posiadają organizacje handlowe i produkcyjne, fundusze ubezpieczeniowe, firmy telekomunikacje, banki, usługi komunalne, urzędy i wiele innych. Warto zwrócić uwagę, że szczególnie wiele certyfikatów



Rys. 1. Liczba akredytowanych certyfikatów ISMS (BS 7799-2) na świecie (stan na grudzień 2005 r.). Źródło: www.xisec.com

posiadają organizacje w państwach wysoko rozwiniętych, niekoniecznie z branży IT, ale dużych wymaganiach technologicznych lub usług profesjonalnych. Wg najnowszych danych, liczba akredytowanych certyfikacji ISMS przekroczyła 2000, jest ich najwięcej w Japonii, Wielkiej Brytanii oraz Indiach. Nie ma jeszcze statystyk wskazujących na certyfikaty zgodności z ISO/ IEC 27001:2005, przede wszystkim z uwagi na trwanie procedur akredytacji jednostek certyfikujących.

DTI Department of Trade and Industry	1993	**DTI Code of Practice**	
BSI British Standards Institution	1995	BS 7799-1:1995	
	1998		BS 7799-2:1998
	1999	BS 7799-1:1999	BS 7799-2:1999
ISO International Standards Organization	2000	ISO/17799:2000	
	2002		BS 7799-2:2002
	2005	ISO/IEC 17799:2005	ISO/IEC 27001:2005
	200?	ISO/IEC 27001:200?	
	200?	ISO/IEC 27002:200?	

Rys. 2 Ewolucja standardów ISMS. Źródło: opracowanie własne

Celowe wydaje się zestawienie danych statystycznych związanych z liczbą certyfikatów z innymi danymi[5], z których wynika że 90% ankietowanych potwierdziło że zarejestrowało incydenty (naruszenie zabezpieczeń informatycznych) w okresie 12 miesięcy; 80% z nich potwierdziło także że pociągnęło to za sobą skutki finansowe dla ich organizacji. Z tej grupy 46% (223 ankietowanych) wyszacowało te straty na poziomie 455.848.000,00 USD[6]. Wyniki badań dowodzą, że temat bezpieczeństwa

[4] T. Humpreys, Improved ISO/ IEC 17799 heralds New series on information security management systems, ISO Management Systems, September – October 2005, s. 27.

[5] Na podstawie 2002 Computer Crime and Security Survey – badaniach przeprowadzonych na próbie 503 instytucji w USA – użytkowników systemów informatycznych. Badanie zostało przeprowadzone przez Computer Security Institute (CSI) we współpracy z San Francisco Dwderal Bureau of Investigation (FBI) Komputer Intrusion Squad.

[6] Business standards: IT Security – securing your business advantage, ISO Management Systems, July – August 2003, s. 36.

informacji wymaga skutecznego nadzorowania przez każdą organizację, bowiem zagraża jej funkcjonowaniu. Odpowiedzią na takie potrzeby od kilku lat są dobre praktyki w zakresie systemowego zarządzania bezpieczeństwem informacji (ISMS). Od wielu lat wiodącą rolę w tym zakresie miały standardy brytyjskie, obecnie rozpoczęła się ich międzynarodowa kariera.

ISO/ IEC 17799:2005 oraz ISO/ IEC 27001:2005 to część serii ISO 27000 rozwijanej przez JTC 1/SC 27. Zgodnie z planem ostatecznie numer pierwszego standardu zostanie zastąpiony przez ISO/ IEC 27002:2007, a obecnie trwają prace nad ISO/IEC 27003 oraz ISO/ IEC 27004, które to dokumenty mają charakter przewodnikowy wobec ISO/ IEC 27001:2005.

Tab. 2 Zmiana numeracji rozdziałów – porównanie BS 7799-2 oraz ISO/ IEC 27001:2005.

BS 7799-2:2002		ISO/IEC 27001:2005	
A3	Polityka bezpieczeństwa	A5	Polityka bezpieczeństwa
A4	Organizacja bezpieczeństwa	A6	Organizacja bezpieczeństwa informacji
A5	Klasyfikacja i kontrola aktywów	A7	Zarządzanie aktywami
A6	Bezpieczeństwo osobowe	A8	Bezpieczeństwo zasobów ludzkich
A7	Bezpieczeństwo fizyczne i środowiskowe	A9	Bezpieczeństwo fizyczne i środowiskowe
A8	Zarządzanie systemami i sieciami	A10	Zarządzanie systemami i sieciami
A9	Kontrola dostępu do systemu	A11	Kontrola dostępu do systemu
A10	Rozwój i utrzymanie systemu	A12	Nabycie systemu informacyjnego, rozwój i utrzymanie
		A13	Zarządzanie incydentami bezpieczeństwa infomacji (przegrupowane pkt. A.6.3.1, A.6.3.2, A.6.3.3, A.6.3.4, A8.1.3, A.12.1.7)
A11	Zarządzanie ciągłością działania	A14	Zarządzanie ciągłością działania
A12	Zgodność	A15	Zgodność

Źródło: Opracowanie własne na podstawie 7799-2 oraz ISO/ IEC 27001:2005

Standardy ISMS zmieniają się niezwykle dynamicznie. Nie jest to na pewno kategoria „problem", skoro celem jest zapewnienie odpowiedniego poziomu bezpieczeństwa. W przypadku certyfikacji jednak, konieczne jest dostosowanie rozwiązań do nowych wymagań, najczęściej wcześniej odpowiadających BS 7799-2, i obecnie ISO/ IEC 27001:2005[7].

Zmiany w najnowszych standardach ISMS

Zgodnie z intencją ISO, wprowadzenie ISO/IEC 27001:2005[8] powinno spopularyzować bardzo ważny aspekt jakości obsługi klienta – bezpieczeństwo informacji. Informacje są atutem, który jak inne temu podobne ważne atuty handlowe, dodaje wartość dla organizacji i wskutek tego wymaga ochrony. Kształtowanie jakości zarządzania w tym zakresie powinno zabezpieczać dane i informacje wobec szerokiego spektrum zagrożeń dla zapewnienia ciągłości działania i w tym obsługi klientów, minimalizowania strat i możliwie szybki powrót w przypadku utraty ciągłości działania. ISMS powinien w indywidualny, adekwatny i skuteczny sposób zapewniać systematyczne podejście do zarządzania informacjami wymagającymi ochrony. A w praktyce stanowi skorelowany z sobą system zabezpieczeń, ustanowionych w odpowiedzi na wcześniej określone ryzyko.

W normie ISO/IEC 27001:2005 znalazło w pełni odzwierciedlenie koncepcji podejścia procesowego, od 2000 roku propagowane w ISO 9001:2000 oraz ISO 14001:2004 oraz założenie ciągłego doskonalenia zgodnego z cyklem PDCA. ISO/IEC 27001:2005 jest istotnym uzupełnieniem wcześniej wydanej normy ISO/IEC 17799:2005. Wobec czego na poziomie międzynarodowym określone zostały zarówno wymagania stanowiące podstawę certyfikacji oraz ich omówienie i przewodnik po realizacji założeń ISMS.

Dla organizacji, które myślą o certyfikacji ISMS, w szczególności dla tych które będą dostosowywały swoje systemy do nowych kryteriów auditowych (ISO/ IEC 27001:2005) ważne jest wskazanie różnic pomiędzy standardem brytyjskim i najnowszym międzynarodowym. Zmiany te dotyczą numeracji poszczególnych rozdziałów i ich nazewnictwa, punktów kontrolnych (zabezpieczeń) – niektóre zostały usunięte inne dodane, a inne zostały przegrupowane.

Praktyka utrzymania i doskonalenia ISMS oraz próba zwiększenia uniwersalności wymagań spowodowała usunięcie niektórych zabezpieczeń, niekiedy jednak okazuje się być to kontrowersyjne. Do takich dyskusyjnych wyłączeń na pewno należy zaliczyć:

- wymagania bezpieczeństwa w umowach zlecania na zewnątrz,

Tab. 3. Usunięte z wymagań ISO/ IEC 27001:2005 zabezpieczenia (punkty kontrolne).

A.4.3.1	Wymagania bezpieczeństwa w umowach zlecania na zewnątrz
A.5.1.6	Zewnętrzne zarządzanie urządzeniami
A.9.4.2	Wymuszenie dróg połączeń
A.9.4.9	Bezpieczeństwo usług sieciowych
A.9.5.1	Automatyczna identyfikacja terminalu
A.9.5.6	Alarm działania pod przymusem do zabezpieczenia użytkowników
A.10.3.2	Szyfrowanie
A.10.3.3	Podpisy cyfrowe
A.10.3.4	Usługi niezaprzeczalności

Źródło: Opracowanie własne na podstawie 7799-2 oraz ISO/ IEC 27001:2005

- wymuszenie dróg połączeń,
- bezpieczeństwo usług sieciowych.

Przy tym jednak oczywiście nadrzędnym celem ISMS jest jego skuteczność i adekwatność do rezultatów szacowania ryzyk, a zatem ww. dziewięć wyłączeń nie niesie ze sobą ryzyka zmniejszenia poziomu bezpieczeństwa. Jest to zagwaran-

[7] Do końca 2005 roku, żadna jednostka certyfikacyjna nie oferowała akredytowanej certyfikacji na zgodność z ISO/ IEC 27001:2005.

[8] ISO/ IEC 27001:2005 został opracowany i będzie rozwijany przez ISO/IEC Joint Technical Committee JTC 1, Information technology, Subcommittee SC 27, Security techniques, Working Group WG 1, Requirements, security services and guidelines.

towane także poprzez rekonfigurację wymaganych punktów kontrolnych, a szczególnie dodanie nowych[9]. Zostały one przytoczone szczegółowo w tab. 4, przedstawiającej osiemnaście (17+1) nowych zabezpieczeń wraz z odniesieniami do wcześniejszej (z normy BS 7799-2) lokalizacji i nazewnictwa.

I wreszcie z formalnego punktu widzenia ważne jest zaprezentowanie także przegrupowań wymaganych zabezpieczeń. Szczególnie istotne z uwagi na konieczność dostosowania Deklaracji stosowania oraz wielu innych dokumentów ISMS, które wcześniej przygotowywano w kontekście BS 7799-2 a wymagają modyfikacji.

[9] ISO/ IEC 27001:2002 wobec organizacji BS 7799-2 zawiera nowe, wymagane zabezpieczenia; odpowiednio: A6 – 1 pkt.; A7 – 2 pkt.; A8 – 4 pkt.; A9 – 1 pkt.; A10 – 8 pkt.; A12 – 1 pkt.; (A13) – (1pkt.).

Tab. 4. Nowe zabezpieczenia w normie ISO/ IEC 27001:2005 (w stosunku do BS 7799-2).

A6	**Organizacja bezpieczeństwa informacji**	
A.6.2 Strony zewnętrzne (dawne A.4.2 Bezpieczeństwo dostępu osób trzecich)		
A.6.2.2 (dawne A.4.2)	Uzgodnienie spraw bezpieczeństwa podczas pracy z klientem	Wszystkie zidentyfikowane wymagania bezpieczeństwa powinny zostać uzgodnione przed udostępnieniem klientom informacji organizacyjnych lub aktywów.
A7	**Zarządzanie aktywami**	
A.7.1 Odpowiedzialność za aktywa (dawne A.5.1 Inwentaryzacja aktywów)		
A.7.1.2	Własność aktywów	Wszystkie aktywa związane z systemem informacji lub usługami powinny mieć swojego właściciela wyznaczonego przez odpowiedni dział organizacji.
A.7.1.3	Akceptowane użycie aktywów	Zasady akceptowalnego użycia aktywów związanych z systemem informacji lub usługami powinny zostać zidentyfikowane, udokumentowane i wdrożone.
A8	**Bezpieczeństwo zasobów ludzkich**	
A.8.2 Strony zewnętrzne *Cel:* Zapewnienie, że wszyscy pracownicy, zleceniobiorcy i użytkownicy stron trzecich są świadomi zagrożeń i potrzeby zabezpieczenia informacji, ich odpowiedzialności i wiarygodności oraz są przygotowani do wspierania polityki bezpieczeństwa instytucji w trakcie ich normalnej pracy i do redukowania ryzyka wystąpienia błędu ludzkiego. (dawne A.6.2 Szkolenie użytkowników)		
A.8.2.1	Zarządzanie odpowiedzialnościami	Zarządzanie powinno wymagać od pracowników, zleceniobiorców i użytkowników stron trzecich stosowania bezpieczeństwa w zgodzie z ustanowionymi politykami i procedurami organizacji.
A.8.3 Wypowiedzenie lub zmiana w zatrudnieniu *Cel:* Zapewnienie, że odejście pracowników, zleceniobiorców i użytkowników stron trzecich z organizacji lub zmiana w zatrudnieniu jest przeprowadzona w zorganizowany sposób.		
A.8.3.1	Wygaśnięcie odpowiedzialności	Odpowiedzialności odprawianego personelu powinny być jasno zdefiniowane i wskazane.
A.8.3.2	Zwrot aktywów	Wszyscy pracownicy, zleceniobiorcy i użytkownicy stron trzecich powinni zwrócić aktywa w siedzibie organizacji na czas wygaśnięcia warunków umowy.
A.8.3.3	Usuwanie praw dostępu	Prawa dostępu wszystkich pracowników, zleceniobiorców i użytkowników stron trzecich do informacji i urządzeń przetwarzających informację powinny zostać usunięte na czas wygaśnięcia warunków umowy lub dostosowane odpowiednio do zmiany.

pracownicy → pracownicy, zleceniobiorcy i użytkownicy stron trzecich

A9	**Bezpieczeństwo fizyczne i środowiskowe**	
A.9.1 Obszary bezpieczne *Cel:* Zapobieganie nieuprawnionemu dostępowi, uszkodzeniom i ingerencji w obiekty instytucji i jej informacje. (dawne A.7.1 Obszary bezpieczne)		
A.9.1.4	Zabezpieczenie przed zewnętrznymi i środowiskowymi zagrożeniami.	Organizacja powinna wskazać i zatwierdzić fizyczne zabezpieczenia bezpieczeństwa przed uszkodzeniami spowodowanymi pożarem, powodzią, trzęsieniem ziemi, wybuchem, niepokojem społecznym lub innymi formami naturalnych bądź przez człowieka wywołanych katastrof.
A10	**Zarządzanie systemami i sieciami**	
A.10.2 Zarządzanie dostawami usług stron trzecich *Cel:* Zapewnienie, że odejście pracowników, zleceniobiorców i użytkowników stron trzecich z organizacji lub zmiana w zatrudnieniu jest przeprowadzona w zorganizowany sposób.		
A.10.2.1	Dostawa usług	Organizacja powinna zapewnić, że zabezpieczenia, definicje usług i poziomy dostaw zawierają w umowach dostaw usług strony trzeciej są wdrożone, obsługiwane i utrzymywane przez stronę trzecią.
A.10.2.2	Monitorowanie i przegląd usług stony trzeciej	Organizacja powinna regularnie monitorować i przeglądać usługi, raporty i zapisy dostarczane przez stronę trzecią i przeprowadzać regularne audity.
A.10.2.3	Zarządzanie zmianami usług strony trzeciej	Organizacja powinna zarządzać zmianami świadczonych usług, włączając w to utrzymywanie i ulepszanie istniejących polityk bezpieczeństwa informacji, procedur i zabezpieczeń, zwracając uwagę na krytyczne procesy biznesowe i ponowne szacowanie ryzyka.
A.10.4 Ochrona przed szkodliwym i mobilnym kodem (mobile code) (dawne A.8.3 Ochrona przed szkodliwym oprogramowaniem)		

A.10.4.1	Zabezpieczenia przed mobilnym kodem	Wprowadzenie mobilnego kodu powinno ograniczać mobilność kodu w dedykowanym środowisku unikając takich kodów, które naruszają organizacyjną politykę bezpieczeństwa informacji.
A.10.6 Zarządzanie bezpieczeństwem sieci (dawne A.8.5 Zarządzanie sieciami)		
A.10.6.2	Bezpieczeństwo usług sieciowych	Cechy bezpieczeństwa, poziomy usług i zarządzanie wymaganiami wszystkich usług sieciowych powinny być zidentyfikowane i włączone w każdą umowę usług sieciowych, nawet jeżeli te usługi są dostarczane do domu lub mają charakter outsourcingu.
A.10.8 Wymiana informacji (dawne A.8.7 Wymiana danych i oprogramowania)		
A.10.8.1	Polityki i procedury wymiany informacji	Formalne polityki, procedury i zabezpieczenia powinny być ustanowione i powinny chronić wymianę informacji poprzez użycie wszystkich typów narzędzi komunikacyjnych.
A.10.9 Bezpieczeństwo handlu elektronicznego *Cel:* Zapewnienie bezpieczeństwa handlu elektronicznego i jego bezpieczne użycie. (nowe z dawnego A.8.7.3)		
A.10.9.2	Transakcje online	Informacja dostarczana w transakcjach Online powinna być chroniona aby zapobiec niekompletnej transmisji, mis-routing, nieautoryzowanej alteracji wiadomości, nieautoryzowanemu ujawnieniu, nieautoryzowanej duplikacji wiadomości lub odtworzeniu.
A.10.10 Monitoring *Cel:* Wykrycie nieautoryzowanych działań A.9.7 Monitorowanie dostępu do systemu i jego użycia (przeniesione z dawnego A.9.7.1-A.9.7.3 i A.8.4.2, A.8.4.3)		
A.10.10.3	Zabezpieczenie log	Urządzenia logging facilities i dzienniki log powinny być chronione przed modyfikacją (tampering) i nieautoryzowanych dostępem.
Nabycie systemu informacyjnego, rozwój i utrzymanie		
A.12.6 Zarządzanie podatnością *Cel:* Zapobiegnięcie szkodom powstałym z wykorzystania publikowanych podatności.		
A.12.6.1	Zabezpieczenie podatności	W porę informacja o podatnościach systemu informacji powinna być otrzymywana. Organizacyjne ujawnienie ocenionych podatności i odpowiednio dokonane pomiary korespondują z ryzykiem.
(Przegrupowane z A.6.3.1, A.6.3.2, A.8.1.3, A.12.1.7)		
Zarządzanie incydentami bezpieczeństwa informacji		
A.13.1 Raportowanie wydarzeń bezpieczeństwa informacji i słabości *Cel:* Zapewnienie że wydarzenia bezpieczeństwa informacji i słabości związane z systemem informacyjnym są zgłaszane w sposób umożliwiający podjęcie w porę działań korygujących.		
A.6.3 Reagowanie na naruszenie bezpieczeństwa i niewłaściwe funkcjonowanie systemu *Cel:* Minimalizowanie strat będących skutkiem naruszenia bezpieczeństwa oraz niewłaściwego funkcjonowania systemu oraz monitorowanie i wyciąganie wniosków z takich przypadków.		

Źródło: Opracowanie własne na podstawie 7799-2 oraz ISO/ IEC 27001:2005

Tab. 5 Zestawienie przegrupowanych zabezpieczeń (punktów kontrolnych) w normie ISO/ IEC 27001:2005 (w stosunku do BS 7799-2).

dawne A.4.1.5	Kontakt ze specjalnymi grupami interesów (przeniesiona do A.6.1.7)
dawne A.4.1.6	Kontakt z władzami (przeniesiona do A.6.1.6)
dawne A.6.1.3	umowa o zachowaniu poufności (przeniesiona do A.6.1.5)
dawne A.6.3.1 A.6.3.2 A.6.3.3 A.6.3.4	(przeniesiona do A.13.1.1 A.13.1.2 A.6.2.2 i A.6.2.3 A.13.2.2)
dawne A.7.3.1	Polityka czystego biurka i czystego ekranu (przeniesiona do A.11.3.3)
dawne A.7.3.2	Wynoszenie mienia (przeniesiona do A.9.2.7)
dawne A.8.1.3	Procedury zarządzania incydentami związanymi z bezpieczeństwem (przeniesiona do A.13.2.1)
dawne A.8.4.2	Dzienniki operatorów (przeniesiona do A.10.10.4)
dawne A.8.4.3	Zapisywanie informacji o błędach (przeniesiona do A.10.10.5)
dawne A.9.7.1	Zapisywanie informacji o zdarzeniach (przeniesiona do A.10.10.1 monitoring)
dawne A.9.7.2	Monitorowanie użycia systemu (przeniesiona do A.10.10.2 monitoring)
dawne A.9.7.3	Synchronizacja zegarów (przeniesiona do A.10.10.6 monitoring)
dawne A.9.5.4	System zarządzania hasłami (przeniesiona do A.11.5.3
dawne A.10.5.4	Wyciek informacji (przeniesiona do A.12.5.4)
dawne A.12.1.7	Gromadzenie materiału dowodowego (przeniesiona do A.13.2.3)

Źródło: Opracowanie własne na podstawie 7799-2 oraz ISO/ IEC 27001:2005

Podobnie można wskazać zmiany jakie zostały dokonane w najnowszej edycji ISO/ IEC 17799:2005. Przy tym jednak oczywiście nie ma konieczności ich przybliżania tak detalicznego jak w przypadku kryteriów auditowych jakie stanowić może ISO/ IEC 27001:2005. Przy tym jednak z uwagi na potencjalne zainteresowanie organizacji definiujących własną politykę bezpieczeństwa bez stawiania celu – certyfikacja ISMS; ISO/ IEC 17799:2005 wydaje się być standardem ważniejszym[10]. Zmiany jakich dokonano w najnowszym wydaniu standardu można scharakteryzować zamierzeniem lepszego dostosowania proponowanych elementów ISMS do

[10] Patrz m.in. T. Humpreys, Improved ISO/ IEC 17799 heralds New series on information security management systems, ISO Management Systems, September – October 2005, s. 28.

Tab. 6 Macierz korelacji BS 7799-2:2002 i ISO/IEC 27001:2005. Źródło: Opracowanie własne na podstawie 7799-2 oraz ISO/ IEC 27001:2005

BS 7799-2:2002	ISO/IEC 27001:2005	BS 7799-2:2002	ISO/IEC 27001:2005	BS 7799-2:2002	ISO/IEC 27001:2005
A.3	A.5	A.8.1.2	A.10.1.2	A.9.5.8	A.11.5.6
A.3.1	A.5.1	A.8.1.3	A.13.2.1	A.9.6	A.11.6
A.3.1.1	A.5.1.1	A.8.1.4	A.10.1.3	A.9.6.1	A.11.6.1
A.3.1.2	A.5.1.2	A.8.1.5	A.10.1.4	A.9.6.2	A.11.6.2
A.4	A.6	A.8.1.6	usunięto	A.9.7	usunięto
A.4.1	A.6.1	A.8.2	A.10.3	A.9.7.1	A.10.10.1
A.4.1.1	A.6.1.1	A.8.2.1	A.10.3.1	A.9.7.2	A.10.10.2
A.4.1.2	A.6.1.2	A.8.2.2	A.10.3.2	A.9.7.3	A.10.10.6
A.4.1.3	A.6.1.3	A.8.3	A.10.4	A.9.8	A.11.7
A.4.1.4	A.6.1.4	A.8.3.1	A.10.4.1	A.9.8.1	A.11.7.1
A.4.1.5	A.6.1.7	A.8.4	A.10.5	A.9.8.2	A.11.7.2
A.4.1.6	A.6.1.6	A.8.4.1	A.10.5.1	A.10	A.12
A.4.1.7	A.6.1.8	A.8.4.2	A.10.10.4	A.11.1	A.12.1
A.4.2	A.6.2	A.8.4.3	A.10.10.5	A.10.1.1	A.12.1.1
A.4.2.1	A.6.2.1	A.8.5	A.10.6	A.10.2	A.12.2
A.4.2.2	A.6.2.2, A.6.2.3	A.8.5.1	A.10.6.1	A.10.2.1	A.12.2.1
A.4.3	usunięto	A.8.6	A.10.7	A.10.2.2	A.12.2.2
A.4.3.1	usunięto	A.8.6.1	A.10.7.1	A.10.2.3	A.12.2.3
A.5	A.7	A.8.6.2	A.10.7.2	A.10.2.4	A.12.2.4
A.5.1	A.7.1	A.8.6.3	A.10.7.3	A.10.3	A.12.3
A.5.1.1	A.7.1.1	A.8.6.4	A.10.7.4	A.10.3.1	A.12.3.1
A.5.2	A.7.2	A.8.7	A.10.8	A.10.3.2	usunięto
A.5.2.1	A.7.2.1	A.8.7.1	A.10.8.2	A.10.3.3	usunięto
A.5.2.2	A.7.2.2	A.8.7.2	A.10.8.3	A.10.3.4	usunięto
A.6	A.8	A.8.7.3	A.10.9.1	A.10.3.5	A.12.3.2
A.6.1	A.8.1	A.8.7.4	A.10.8.4	A.10.4	A.12.4
A.6.1.1	A.8.1.1	A.8.7.5	A.10.8.5	A.10.4.1	A.12.4.1
A.6.1.2	A.8.1.2	A.8.7.6	A.10.9.3	A.10.4.2	A.12.4.2
A.6.1.3	A.6.1.5	A.8.7.7	usunięto	A.10.4.3	A.12.4.3
A.6.1.4	A.8.1.3	A.9	A.11	A.10.5	A.12.5
A.6.2	usunięto	A.9.1	A.11.1	A.10.5.1	A.12.5.1
A.6.2.1	A.8.2.2	A.9.1.1	A.11.1.1	A.10.5.2	A.12.5.2
A.6.3	usunięto	A.9.2	A.11.2	A.10.5.3	A.12.5.3
A.6.3.1	A.13.1.1	A.9.2.1	A.11.2.1	A.10.5.4	A.12.5.4
A.6.3.2	A.13.1.2	A.9.2.2	A.11.2.2	A.10.5.5	A.12.5.5
A.6.3.3	usunięto	A.9.2.3	A.11.2.3	A.11	A.14
A.6.3.4	A.13.2.2	A.9.2.4	A.11.2.4	A.11.1	A.14.1
A.6.3.5	A.8.2.3	A.9.3	A.11.3	A.11.1.1	A.14.1.1
A.7	A.9	A.9.3.1	A.11.3.1	A.11.1.2	A.14.1.2
A.7.1	A.9.1	A.9.3.2	A.11.3.2	A.11.1.3	A.14.1.3
A.7.1.1	A.9.1.1	A.9.4	A.11.4	A.11.1.4	A.14.1.4
A.7.1.2	A.9.1.2	A.9.4.1	A.11.4.1	A.11.1.5	A.14.1.5
A.7.1.3	A.9.1.3	A.9.4.2	usunięto	A.12	A.15
A.7.1.4	A.9.1.5	A.9.4.3	A.11.4.2	A.12.1	A.15.1
A.7.1.5	A.9.1.6	A.9.4.4	A.11.4.3	A.12.1.1	A.15.1.1
A.7.2	A.9.2	A.9.4.5	A.11.4.4	A.12.1.2	A.15.1.2
A.7.2.1	A.9.2.1	A.9.4.6	A.11.4.5	A.12.1.3	A.15.1.3
A.7.2.2	A.9.2.2	A.9.4.7	A.11.4.6	A.12.1.4	A.15.1.4
A.7.2.3	A.9.2.3	A.9.4.8	A.11.4.7	A.12.1.5	A.15.1.5
A.7.2.4	A.9.2.4	A.9.4.9	usunięto	A.12.1.6	A.15.1.6
A.7.2.5	A.9.2.5	A.9.5	A.11.5	A.12.1.7	A.13.2.3
A.7.2.6	A.9.2.6	A.9.5.1	usunięto	A.12.2	A.15.2
A.7.3	usunięto	A.9.5.2	A.11.5.1	A.12.2.1	A.15.2.1
A.7.3.1	A.11.3.3	A.9.5.3	A.11.5.2	A.12.2.2	A.15.2.2
A.7.3.2	A.9.2.7	A.9.5.4	A.11.5.3	A.12.3	A.15.3
A.8	A.10	A.9.5.5	A.11.5.4	A.12.3.1	A.15.3.1
A.8.1.	A.10.1	A.9.5.6	usunięto	A.12.3.2	A.15.3.2
A.8.1.1	A.10.1.1	A.9.5.7	A.11.5.5		

współczesnej organizacji działającej we współczesnym otoczeniu. Nacisk jaki został położony w omawianym standardzie koncentruje się m.in. na bezpieczeństwie na styku współdziałających w różnym charakterze organizacji, zarządzanie incydentami, szacowaniu ryzyk i korelacja działań podejmowanych w odniesieniu do rezultatów, urządzeń mobilnych, łączności bezprzewodowej, zarządzaniu kadrami w aspektach bezpieczeństwa informacji.

Tab. 7 Porównanie układów norm ISO/ IEC 17799:2002 oraz ISO/ IEC 17799:2005.

ISO/IEC 17799:2002	ISO/IEC 17799:2005
Polityka bezpieczeństwa	Polityka bezpieczeństwa
Organizacja bezpieczeństwa	Organizacja bezpieczeństwa informacji
Klasyfikacja i kontrola aktywów	Zarządzanie aktywami
Bezpieczeństwo osobowe	Bezpieczeństwo zasobów ludzkich
Bezpieczeństwo fizyczne i środowiskowe	Bezpieczeństwo fizyczne i środowiskowe
Zarządzanie systemami i sieciami	Zarządzanie systemami i sieciami
Kontrola dostępu	Kontrola dostępu
Rozwój i utrzymanie systemu	Ustanowienie, rozwój i utrzymanie systemu
---	Zarządzanie incydentami bezpieczeństwa informacji
Zarządzanie ciągłością działania	Zarządzanie ciągłością działania
Zgodność	Zgodność

Źródło: Opracowanie własne na podstawie ISO/ IEC 17799:2002 oraz ISO/ IEC 17799:2005.

W najnowszym standardzie ISO/ IEC 17799:2005 wskazane zostały krytyczne – z uwagi na bezpieczeństwo informacji – czynniki sukcesu dotyczące zarządzania. Zostały one odniesione m.in. do strategii, organizacji bezpieczeństwa, kadr, dostępów, rozwiązań systemowych, ciągłości działania, uczenia się na incydentach. Do najważniejszych dokonanych zmian należy zaliczyć:

- zwrócenie szczególnej uwagi na ryzyka i zagrożenia – ich roli w zarządzaniu,
- podkreślenie wzrastającej roli współpracy outsourcingowej w działalności gospodarczej typowej organizacji,
- nowe technologie oraz związane z nimi nowe relacje wewnątrzsystemowe i ryzyka jakie generują,
- konieczność znajomości i spełnienia wymagań coraz większej liczby bardzo zróżnicowanych wymagań – regulacji zewnętrznych (od prawa różnych szczebli do wymagań klientów).

W efekcie w najnowszych wydaniach standardów ISO/ IEC, zgodnie z założeniami zapewniono także harmonizację podejścia i terminów z istotnymi dla wdrażania, utrzymania i doskonalenia ISMS:

- ISO Guide 73 (Pism Management Vocabulary,
- ISO/ IEC TR 13335 Guidelines for the Management of IT Security,
- ISO/ IEC TR 18044 Information Security Incydent Management.

Podsumowanie

ISO/IEC 27001:2005 może zostać wykorzystana jako podstawa ISMS przez dowolną organizację, niezależnie od wielkości, formy prawnej, czy branży. Przy czym już dotychczasowa praktyka dowodzi, że skuteczne zastosowanie zabezpieczeń, jakie przywołuje standard wymaga wielu nakładów finansowych i zmian organizacyjnych. Trudno wobec tego zakładać, że certyfikowane ISMS to dostępna droga do zapewnienia bezpieczeństwa informacji dla każdej organizacji. Przy tym jednak na pewno benchmarking w tym zakresie i ew. adaptacja rozwiązań to najkorzystniejsze rozwiązanie. A właśnie omawiane standardy są takim zbiorem najlepszych praktyk, nawet jeżeli celem nie jest certyfikacja ISMS.

Ustanowienie, udokumentowanie i wdrożenie ISMS, jego certyfikacja w oparciu o ISO/IEC 27001:2005 jest na pewno dowodem dla klientów i dostawców, że w ramach systemu zarządzania dokonana została ocena ryzyka związanego z informacją i na podstawie rezultatów kształtowane są właściwe rozwiązania. Deklaracja stosowania[11] – kluczowy, wynikowy dokument w systemie zarządzania bezpieczeństwem informacji dostępny dla wszelkich zainteresowanych stron informuje o zastosowanych zabezpieczeniach i coraz częściej, podobnie jak księga jakości, jest wymagana przy zawieraniu istotnych kontraktów.

Dane i informacje zaliczane są do zasobów o charakterze krytycznym dla prowadzonej działalności, stanowią lub determinują wartość dodaną w aktywności każdej organizacji i dlatego wymagają szczególnej troski – właściwego zarządzania i ochrony. Ostatecznie standardy: ISO/ IEC 17799:2005 oraz ISO/ IEC 27001:2005 stanowią komplementarną parę. Wykorzystanie zawartych w nich wymagań i wytycznych ma na celu podniesienie poziomu bezpieczeństwa informacji i może przybrać postać certyfikowanego systemu zarządzania (ISO/ IEC 27001:2005). Fakt umiędzynarodowienia standardów w tym zakresie na pewno będzie sprzyjał upowszechnieniu zasad systemowego zarządzania bezpieczeństwem informacji. Przy tym niektóre jednostki certyfikujące informują o stosunkowo krótkim czasie (sześciu miesięcy) koniecznego dostosowania certyfikowanych ISMS na zgodność z BS 7799-2, do wymagań nowego, międzynarodowego standardu ISO/ IEC 27001:2005.

Literatura:

1. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.
2. ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management.
3. T. Humpreys, Improved ISO/ IEC 17799 heralds New series on information security management systems, ISO Management Systems, September – October 2005.
4. Business standards: IT Security – securing your business advantage, ISO Management Systems, July – August 2003.
5. www.xisec.com

[11] Deklaracja stosowania (Statement of Applicability) jest wymaganym w ISO/ IEC 27001:2005 dokumentem. Patrz p. 4.2.1 j.). W swojej treści powinno być to zestawienie celów oraz stosowanych w ramach ISMS zabezpieczeń, wskazaniem przyczyn ich aplikacji oraz ew. wyłączeń i ich uzasadnień.