Anna Bielawa

System zarządzania bezpieczeństwem informacji według normy ISO

Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania 1, 171-176

2008

STUDIA I PRACE WYDZIAŁU NAUK EKONOMICZNYCH
I ZARZĄDZANIA NR 1

ANNA BIELAWA

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI WEDŁUG NORMY ISO/IEC 27001:2005

Informacja jest jednym z ważniejszych narzędzi uzyskania przewagi konkurencyjnej. Coraz szybszy rozwój techniki w bardzo dużym stopniu zależy od szybkości i jakości informacji. Informacja i wspierające ją procesy, systemy i sieci są ważnymi aktywami biznesowymi. Wraz z rozwojem technik komunikacji pojawiają się nowe sposoby uzyskiwania informacji, będących tajemnicami ważnymi z punktu widzenia organizacji. Coraz częściej organizacje, ich systemy i sieci informatyczne są narażone na zagrożenia zamierzone, takie jak szpiegostwo, sabotaż, wandalizm, bądź niezamierzone, do których można zaliczyć brak świadomości pracowników, pożar lub powódź. Uzależnienie instytucji od systemów i usług informacyjnych oznacza, że są bardziej podatne na zagrożenia utraty bezpieczeństwa, dlatego tak ważne jest zapewnienie bezpieczeństwa informacji. Do tematu tego można podejść na wiele sposobów. Mogą to być działania wyrywkowe, nieskoordynowane i intuicyjne, uzależniające bezpieczeństwo informacji od poziomu wiedzy osób, którym powierzono to zadanie. Efekty takich działań mogą zabezpieczyć pewne obszary instytucji, jednak pozostałe mogą być nadal narażone na zagrożenia. Instytucja, która chce należycie zabezpieczyć swoje informacje, powinna zastosować podejście systemowe, polegające na kompleksowym zarządzaniu posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem związanym z bezpieczeństwem informacji.

1. Norma BS-7799 a norma ISO 27001

Norma ISO 27001 jest oparta na brytyjskiej normie BS-7799-2, lecz wprowadzono do niej wiele zmian, które należy uwzględnić przy budowie i utrzymywaniu systemu bezpieczeństwa. Zgodnie ze zmienionymi zasadami akredytacji, certyfikaty BS-7799 nie są przyznawane od 24 lipca 2006 roku, a wszystkie nowe systemy bezpieczeństwa są certyfikowane na zgodność z wymaganiami standardu ISO 27001. W instytucjach posiadających certyfikat BS-7799 powinno podczas audytu lub recertyfikacji nastąpić przejście do nowej normy. Oznacza to, że firmy, które obecnie mają certyfikat BS-7799, podczas najbliższego audytu będą podlegały weryfikacji według zapisów normy ISO 27001.

Zmiana normy BS-7799 nastąpiła pod wpływem jej krytyki, głównie za trudności interpretacyjne i niejasności, niemożność zastosowania jej przez małe i średnie przedsiębiorstwie (problemy z uwzględnieniem pewnych wymagań) i nieodzwierciedlanie dużej dynamiki rozwoju w zakresie IT.

Standard ISO 27001 składa się z części podstawowej i załączników. W części podstawowej normy zdefiniowano wymagania związane z ustanowieniem i zarządzaniem systemem zarządzania bezpieczeństwem informacji, dokumentacją, odpowiedzialnością kierownictwa, wewnętrznymi audytami, przeglądami i ciągłym doskonaleniem systemu. Zmiany wprowadzone do głównej części normy dotyczyły przede wszystkim doprecyzowania i rozszerzenia wymagań związanych z pętlą ciągłego doskonalenia (PDCA). W obecnej wersji norma wymaga na przykład udokumentowania metodyki analizy ryzyka, a także zapewnienia jej powtarzalności i porównywalności wyników. Nie jest to duża zmiana, gdyż dokumentowanie metodyki analizy ryzyka było zazwyczaj jednym z podstawowych etapów dotychczasowych wdrożeń BS 7799-2.

Załącznik A normy ISO/IEC 27001 został poważnie zmieniony – zmodyfikowano układ rozdziałów, część wymagań usunięto bądź pogrupowano, dodano także kilka nowych wymagań. Zarządzanie incydentami bezpieczeństwa stało się jednym z głównych obszarów normy. Załącznik A tej normy wyróżnia zabezpieczenia 11 obszarów wpływających na bezpieczeństwo informacji w organizacji, czyli[1]:

- politykę bezpieczeństwa,
- organizację bezpieczeństwa informacji,

[1] http://globaleconomy.pl/content/view/2183/57/.

- zarządzanie aktywami,
- bezpieczeństwo zasobów ludzkich,
- bezpieczeństwo fizyczne i środowiskowe,
- zarządzanie systemami i sieciami,
- kontrolę dostępu,
- pozyskiwanie, rozwój i utrzymanie systemów informatycznych,
- zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- zarządzanie ciągłością działania,
- zgodność.

Dużą zaletą normy jest kompleksowe podejście do bezpieczeństwa informacji. Wymieniono w niej obszary bezpieczeństwa fizycznego, osobowego, teleinformatycznego i prawnego. Nie określono szczegółowych technicznych wymagań, lecz wskazano na zagadnienia, które należy uregulować. Sposób zabezpieczenia tych obszarów, zależny od przedsiębiorstw, powinien być oparty na przeprowadzonej analizie ryzyka. Ze względu na kompleksowe podejście do tematu bezpieczeństwa informacji i ogólny charakter wymagań norma może być podstawą do budowy systemu zarządzania bezpieczeństwem informacji w organizacjach.

Z normą ISO 2007 związane są następujące normy[2]:

- BS-7799-2:2002 – standard brytyjski, na którego podstawie opracowano normę ISO/IEC 27001:2005,
- PN-ISO/IEC 27001:2007 – polskie tłumaczenie normy ISO/IEC 27001:2005,
- ISO/IEC 17799:2005 – norma zawierająca wytyczne do tego, w jaki sposób spełnić poszczególne wymagania normy ISO/IEC 27001:2005.

2. Korzyści z wdrożenia systemu zarządzania bezpieczeństwem informacji według normy ISO 27001:2005

Zastosowanie normy pozwala określić wymagania przedsiębiorstwa w zakresie bezpieczeństwa, sformułować politykę ochrony i bezpieczeństwa informacji i wybrać środki, dzięki którym zostanie zapewnione bezpieczeństwo informacji. Norma wspomaga więc procesy organizacyjne w sposób umożliwia-

[2] http://centrum.bezpieczenstwa.pl/content/view/51/16/.

jący racjonalne podwyższenie bezpieczeństwa informacji, koncentrując się na sferze organizacyjnej i kontrolując obszary zwiększonego ryzyka, takie jak[3]:

a) dostępność, czyli zapewnienie, że upoważnione osoby mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne;
b) integralność, czyli zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania;
c) poufność, czyli zapewnienie dostępu do informacji tylko upoważnionym osobom.

Dostępność, integralność i poufność informacji ma podstawowe znaczenie dla:

- utrzymania i zwiększenia konkurencyjności,
- zgodności z przepisami prawa (np. ustawa o ochronie danych osobowych i jej pochodnych),
- wydajności (skuteczności działania),
- płynności finansowej,
- rentowności,
- wizerunku firmy.

Zastosowanie wytycznych normy umożliwia zmniejszenie do minimum ryzyka zafałszowania, a nawet utraty informacji, co na obecnym etapie rozwoju technicznego jest niemal koniecznością. Normę można z powodzeniem wdrażać zarówno w przedsiębiorstwach jak i urzędach. W tabeli 1 przedstawiono korzyści ze stosowania tych norm.

W Polsce system ten cieszy się coraz większym uznaniem. Pierwszy, zakończony sukcesem i potwierdzony certyfikatem audyt, przeszła firma Inforsys Sp. z o.o., ekspert usług outsourcingowych z zakresu masowego przetwarzania dokumentów. Drugi certyfikat, ale pierwszy dla urzędu przyznano Urzędowi Miasta Piotrków Trybunalski, a pierwszym bankiem, który może pochwalić się certyfikatem ISO 27001, jest bank PKO BP.

Znaczenie informacji oraz wspierających ją procesów, systemów i sieci stale rośnie, głównie dlatego, że są one ważnymi aktywami biznesowymi. Poufność, dostępność i integralność informacji może mieć podstawowe znaczenie dla utrzymania konkurencyjności, płynności finansowej, zysku i zgodności z przepisami prawa i wizerunku instytucji. Informacja jest głównym czynnikiem rozwoju firm, ale gdy jest niewłaściwie zabezpieczona, może być powodem ich upadku. W dobie postępującej informatyzacji niezbędne jest sformu-

[3] http://www.kema.pl/index.php?iw=331.

łowanie takiej polityki bezpieczeństwa firmy, która uwzględni wszystkie aspekty zarządzania bezpieczeństwem informacji. Dzięki temu klienci mają gwarancję, że utrzymywane w organizacji dane są właściwie zabezpieczone, a skuteczne techniki zabezpieczania informacji są stosowane na każdym poziomie w organizacji. Zadanie to ułatwia norma ISO 27001:2005, która weszła w życie 15 października 2005 roku. Jej wdrożenie to nie tylko moda i cenny dokument, ale również i przede wszystkim wymóg nowoczesnej gospodarki, w której działają organizacje.

Tabela 1

Korzyści wynikające z wdrożenia i funkcjonowania systemu zarządzania bezpieczeństwem informacji według normy ISO 27001:2005 w firmach i urzędach

Grupa docelowa		Korzyść
firma	urząd	
+	+	Spełnienie wymagań ustawowych: – Ustawa o ochronie danych osobowych – Ustawa o ochronie informacji niejawnych – Ustawa o dostępie do informacji publicznej – Ustawa o prawie autorskim i prawach pokrewnych
+	+	Uniknięcie kar za naruszenie bezpieczeństwa informacji
+	+	Ochrona informacji znajdujących się w obiegu w ramach instytucji
+	+	Zabezpieczenie informacji na wypadek katastrof lub awarii – zarządzanie ciągłością działania urzędu
+	+	Uporządkowanie informacji przetwarzanych przez urząd
+	+	Wzrost świadomości pracowników co do bezpieczeństwa informacji
	+	Zapewnienie interesantów i zainteresowane instytucje, że ich dane są właściwie chronione
+		Zapewnienie klientów, że ich informacje znajdują się pod właściwą ochroną
+		Wymagania przetargowe
+		Wiarygodność firmy dla klienta
+	+	Zarządzanie ciągłością działania
+	+	Spełnienie wymagań prawnych dotyczących bezpieczeństwa informacji obowiązujących urząd i ustalenie polityki bezpieczeństwa informacji
+	+	Oszacowanie ryzyka związanego z zarządzaniem informacją
+	+	Organizacja bezpieczeństwa fizycznego i informatycznego informacji
+	+	Zarządzanie systemami informatycznymi i sieciami komputerowymi pod kątem bezpieczeństwa informacji
+	+	Wprowadzenie okresowych audytów bezpieczeństwa informacji
+	+	Ustalenie w formie procedur sposobu postępowania w trakcie normalnego funkcjonowania i sytuacjach kryzysowych

Źródło: http://www.aste.net.pl/szbi/bezpieczenstwo_informacji_korzysci.php.

INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON ISO/IEC 27001:2005

Summary

Information is critical to the operation and perhaps even the survival of the organizations. Being certified to ISO/IEC 27001 will help to manage and protect the valuable information assets. ISO/IEC 27001 is the only auditable international standard which defines the requirements for an Information Security Management System (ISMS). The standard is designed to ensure the selection of adequate and proportionate security controls. It adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the ISMS. ISO/IEC 27001 is suitable for any organization, large or small, in any sector or part of the world. The standard is particularly suitable where the protection of information is critical, such as in the finance, health, public and IT sectors. It's also highly effective for organizations which manage information on behalf of others, such as IT outsourcing companies: it can be used to assure customers that their information is being protected.

Translated by Anna Bielawa