PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 159

Informatyka Ekonomiczna 19 2011

Artur Rot
Uniwersytet Ekonomiczny we Wrocławiu

INSTYTUCJONALIZACJA I STANDARYZACJA ZARZĄDZANIA RYZYKIEM W SYSTEMIE BEZPIECZEŃSTWA INFORMACJI W PRZEDSIĘBIORSTWIE

Streszczenie: Współczesne systemy informacyjne są często bardzo skomplikowane, heterogeniczne i mają charakter dynamiczny. Postęp technologiczny oraz szerokie zastosowanie systemów informatycznych w biznesie generują zależności, które wywołują wzrost różnorodności, złożoności, nieokreśloności i ilości czynników ryzyka. Dlatego coraz większego znaczenia nabiera problematyka zarządzania ryzykiem, koncentrująca się na poszukiwaniu optymalnego stosunku między zagrożeniami a kosztem zabezpieczeń. W artykule zaprezentowane zostały wybrane standardy bardzo dynamicznie rozwijającej się dziedziny, jaką jest zarządzanie ryzykiem na potrzeby bezpieczeństwa informacji w organizacji. Zaprezentowane zostały zarówno najważniejsze międzynarodowe normy ISO/IEC, jak i wybrane dobre praktyki w tym obszarze.

Słowa kluczowe: zarządzanie ryzykiem, bezpieczeństwo systemów informatycznych, standardy ISO/IEC, COBIT.

1. Wstęp

Systemy informatyczne (SI) obejmują coraz to szersze obszary funkcjonowania współczesnych organizacji. Technologia informacyjna pozwala organizacjom osiągnąć nową jakość funkcjonowania, jednocześnie rośnie stopień zdeterminowania sprawnego zarządzania od nowoczesnych i bezpiecznych rozwiązań teleinformatycznych. Współczesne systemy informatyczne są często bardzo skomplikowane, heterogeniczne i mają charakter dynamiczny. Wykreowały one nowe rodzaje ryzyka, a ich bezpieczeństwo nabrało wymiaru globalnego. Obecnie same zabezpieczenia technologiczne nie są już wystarczające, należy optymalnie dobierać różnorodne środki i metody zabezpieczeń, właściwie je stosować oraz wreszcie odpowiednio zarządzać ryzykiem w obszarze bezpieczeństwa informacji i systemów informatycznych. Nowoczesne przedsiębiorstwo musi stosować cały zestaw uzupełniających się produktów, polityk oraz procedur, aby ograniczać ryzyko utraty poufności, integralności i dostępności tych systemów. Ponieważ nie można całkowicie uniknąć ryzyka, należy poznać rządzące nim mechanizmy i odpowiednio nim zarządzać. W tym celu

warto, a wręcz należy korzystać ze światowych norm, standardów, zaleceń i dobrych praktyk w tym zakresie.

Celem niniejszego artykułu jest prezentacja bieżącego stanu zorganizowania oraz standaryzacji bardzo dynamicznie rozwijającej się dziedziny, jaką jest zarządzanie ryzykiem na potrzeby bezpieczeństwa informacji w organizacji. Zaprezentowane zostaną zarówno ważniejsze standardy opracowane przez ISO/IEC, jak i standard COBIT jako przykład zbioru zaleceń i dobrych praktyk w tym obszarze.

2. Wprowadzenie do problematyki zarządzania ryzykiem

Ryzyko towarzyszy człowiekowi i jego działalności od początku dziejów. Od najdawniejszych czasów głównym źródłem ryzyka dla człowieka były żywioły przyrody, takie jak trzęsienia ziemi, powodzie, nawałnice, huragany, nieprzewidywalne oraz ponadprzeciętne upały, susze czy mrozy. Drugim zasadniczym źródłem ryzyka towarzyszącym człowiekowi jest aktywność ludzi. W wyniku rozwoju cywilizacji, kultury, nauki, organizacji, techniki, gospodarki i innych dziedzin powstają nowe obszary działalności człowieka, które stale generują nowe rodzaje ryzyka [Ronka-Chmielowiec (red.) 2004, s. 11]. Do przyspieszenia tempa zmian przyczynia się głównie postęp technologiczny. Ma on skokowy charakter, a zależności, które generuje, wywołują wzrost różnorodności, złożoności, nieokreśloności oraz ilości czynników ryzyka.

Zdefiniowanie ryzyka jest zadaniem bardzo trudnym, a podanie jednoznacznej, precyzyjnej definicji jest wręcz niemożliwe. Ryzyko jest definiowane w różnych naukach i teoriiach, m.in. w ekonomii, naukach behawioralnych, naukach prawnych, psychologii, statystyce, ubezpieczeniach, teorii prawdopodobieństwa i wielu innych. Nauka o ryzyku jest praktycznie rozwijana w większości dziedzin naukowych. Obecnie nie istnieje jeszcze jednolita teoria ryzyka. Jak pisze M. Krupa, ryzyko możemy rozpatrywać na wielu poziomach i niemalże we wszystkich dziedzinach działalności człowieka. W zależności od autora i charakteru opracowania czy też ze względu na perspektywę przedmiotową, branżową lub dyscyplinarną uzyskujemy różne sposoby ujmowania zagadnienia związanego z ryzykiem [Krupa 2002, s. 15].

Również w odmiennych formach działalności biznesowej będziemy mieli do czynienia z indywidualnymi formami ryzyka. Inne typy ryzyka wystąpią przecież w przedsiębiorstwie produkcyjnym, inne natomiast w sektorze finansowym. Oto kilka najczęściej stosowanych definicji ryzyka [Ronka-Chmielowiec (red.) 2009, s. 11]:

- Ryzyko jako szansa wystąpienia straty – szansa straty rozumiana jest jako możliwość/prawdopodobieństwo/stopień prawdopodobieństwa, że zdarzy się sytuacja wywołująca stratę.
- Ryzyko jako możliwość wystąpienia straty – możliwość rozumiana jest w ten sposób, iż wartość prawdopodobieństwa wystąpienia określonego zdarzenia generującego stratę jest zawarta między zerem a jednością.

- Ryzyko jako stan, w którym istnieje możliwość straty – przez ryzyko rozumie się stan rzeczywistości, w której może wystąpić zdarzenie powodujące stratę, czyli może pojawić się wynik inny niż zakładano wcześniej.
- Ryzyko jako prawdopodobieństwo wyniku innego niż oczekiwany – ryzyko rozumiane jest jako obiektywne prawdopodobieństwo, że faktyczny rezultat będzie różnić się od zakładanego.
- Ryzyko jako dyspersja rezultatów rzeczywistych i oczekiwanych – pochodząca ze statystyki definicja, ujmująca ryzyko jako stopień „rozrzutu" wyników w stosunku do pozycji centralnych lub średnich.
- Ryzyko jako przedmiot ubezpieczenia – ryzyko utożsamiane jest z przedmiotem ubezpieczenia, którym mogą być dobra osobiste, majątkowe.

W aspekcie bezpieczeństwa systemów informatycznych ryzyko traktuje jako zbiorczą miarę prawdopodobieństwa i wagi sytuacji, w której dane zagrożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie aktywów systemu informacyjnego, a zatem pośrednią lub bezpośrednią szkodę dla instytucji [ISO 13335-1]. W tym kontekście zarządzanie ryzykiem jest procesem, który przyczynia sie przede wszystkim do zidentyfikowania ryzyka w zakresie utraty poufności, dostępności i integralności. Zidentyfikowane ryzyko zostaje ocenione pod kątem konsekwencji biznesowych oraz oszacowane zostaje prawdopodobieństwo jego wystąpienia. W ramach procesu zarządzania ryzykiem definiuje się zasady i przepisy w zakresie postępowania z ryzykiem, określane również są priorytety podejmowanych działań, których celem jest ograniczanie i eliminowanie ryzyka oraz ciągłe monitorowanie ich efektywności i skuteczności. Dzięki informowaniu o możliwym ryzyku oraz szkoleniom dotyczącym zasad jego ograniczania, systemy informatyczne organizacji i przetwarzane w nich informacje stają się bezpieczniejsze, na czym zyskuje oczywiście cała organizacja [Abramczyk 2008].

3. Instytucjonalizacja zarządzania ryzykiem w aspekcie bezpieczeństwa systemów informatycznych

Problematyka ryzyka dostrzegana była już w pierwszych traktatach ekonomicznych, choć oczywiście podejście do tego zagadnienia było zupełnie odmienne niż obecnie. Od czasu owych pierwszych prób włączenia ryzyka do teorii ekonomicznych nastąpił silny rozwój teorii ryzyka oraz zarządzania ryzykiem w przedsiębiorstwach. Korzystając ze wzrastającej mocy obliczeniowej komputerów oraz powstawania nowych narzędzi matematycznych, ekonomiści przetwarzali coraz więcej informacji, aby określić miary ryzyka. Istnieje wiele instytucji, które miały istotny wpływ na kształtowanie się teorii ryzyka i stymulowały rozwój nowej interdyscyplinarnej dziedziny – zarządzania ryzykiem, nauki z pogranicza zarządzania i nauk ekonomicznych. Wśród najważniejszych wymienić można europejskie stowarzyszenie FERMA – Federation of European Risk Management Associations, federację zrzeszająca menedżerów zajmujących się problematyką ryzyka.. W Polsce członkiem federacji jest

stowarzyszenie POLRISK. W 1980 r. w Stanach Zjednoczonych utworzone zostało towarzystwo SRA (The Society of Risk Analysis), zrzeszające przedstawicieli nauki, świata polityki i ochrony środowiska. Od tego momentu wydawane jest czasopismo „Risk Analysis". Towarzystwo skupia ponad 2500 członków i koncentruje się na propagowaniu problematyki zarządzania ryzykiem. W 1986 r. w Londynie rozpoczął funkcjonowanie Institute for Risk Management. Dziesięć lat później powstało stowarzyszenie GARP (The Global Association of Risk Professionals), skupiające menedżerów ryzyka kredytowego, walutowego, inwestycji kapitałowych. Tego typu instytucji zajmujących się i propagujących problematykę zarządzania ryzykiem jest oczywiście dużo więcej. Są one również źródłem standardów, zaleceń i dobrych praktyk dla organizacji gospodarczych. Również metody i techniki zabezpieczeń systemów informatycznych są przedmiotem standaryzacji, zarówno międzynarodowych, jak i krajowych instytucji standaryzacyjnych. Instytucje te poświęcają coraz więcej uwagi problematyce związanej z zarządzaniem ryzykiem, a w szczególności ryzykiem związanym z bezpieczeństwem systemów informatycznych w organizacjach. Widoczna jest również pewna tendencja, objawiająca się tym, iż kwestie związane z bezpieczeństwem systemów informatycznych, które jeszcze niedawno były traktowane niezależnie, rozpatrywane są coraz częściej w kontekście kompleksowego procesu zarządzania ryzykiem. Te zagadnienia już dawno zostały zauważone przez kierownictwo wielkich koncernów, których troska o bezpieczeństwo funkcjonowania zaowocowała korporacyjnymi standardami w dziedzinie bezpieczeństwa. Na tym gruncie powstało wiele oficjalnych norm, które standaryzują procesy związane z zarządzaniem ryzykiem na potrzeby bezpieczeństwa SI. Czołową organizacją w dziedzinie standaryzacji norm bezpieczeństwa była najstarsza na świecie instytucja normalizacyjna – BSI (British Standards Institution) [*Historia*… 2005].

Wyróżnić można dwa zasadnicze rodzaje norm w omawianym obszarze [Białas 2006, s. 45-46]:

- oficjalne, tworzone przez gremia standaryzacyjne: międzynarodowe (np. ISO, IEC, ITU-T), regionalne (np. CEN, ETSI, NAFTA, APEC) i krajowe (np. ANSI, SCC, NIST, PKN),
- pozostałe standardy, obejmujące zalecenia firm, stowarzyszeń branżowych, organizacji, takich jak ISACA (Information Systems Audit and Control Association), IETF (Internet Engineering Task Force), GAO (US General Accounting Office) czy BSI (Bundesamt fuer Sicherheit in der Informationstechnik). Instytucje te zajmują się opracowywaniem wytycznych, dobrych praktyk (ang. *best practices*), związanych również z problematyką ryzyka informatycznego. Przykładem może być stowarzyszenie ISACA oraz IT Governace Institute. Instytucje te opracowały standard COBIT, stanowiący zbiór dobrych praktyk.
- Wiele standardów w zakresie zarządzania ryzykiem na potrzeby bezpieczeństwa systemów informatycznych opracowanych zostało przez ISO. Celem tej Międzynarodowej Organizacji Standaryzacyjnej jest tworzenie i promowanie norm międzynarodowych w różnorodnych dziedzinach działalności technicznej, eko-

nomicznej i naukowej. W 1987 roku organizacja ta wraz z Międzynarodową Komisją Elektrotechniczną (IEC) utworzyła Połączony Komitet Techniczny nr 1 (JTC 1), którego celem jest tworzenie norm w obszarze IT, a co za tym idzie − także w zakresie ryzyka generowanego przez współczesne systemy informatyczne. Obecnie ISO i IEC tworzą wyspecjalizowany system normalizacji międzynarodowej. Normy i raporty techniczne w obszarze techniki informatycznej, opracowane przez Komitet Techniczny, dostarczają wskazówek i wytycznych osobom zarządzającym bezpieczeństwem informacji, uwzględniają też problemy zarządzania, a w szczególności analizy ryzyka [Szczepankiewicz, Szczepankiewicz 2006]. Na bazie standardów ISO/IEC powstały polskie odpowiedniki tych norm międzynarodowych, odnoszące się bezpośrednio lub pośrednio do bezpieczeństwa informacji, ze szczególnym uwzględnieniem problematyki zarządzania ryzykiem, wydane przez Polski Komitet Normalizacyjny.

W Stanach Zjednoczonych standaryzacją w omawianym obszarze zajmują się przede wszystkim ANSI (American National Standards Institute), NIST (National Institute of Standards and Technology), IEEE (Institute of Electrical and Electronic Engineers). Warto zwrócić uwagę na organizację NIST, która opracowała metodykę zarządzania ryzykiem NIST SP 800-30, opublikowaną pod nazwą *Special Publication 800–30 Risk Management Guide for Information Technology Systems*. Stała się ona obecnie swego rodzaju standardem [Stoneburner i in. 2002]. Zgodnie z wytycznymi zawartymi w metodyce NIST SP 800–30 proces zarządzania ryzykiem składa się z trzech następujących po sobie etapów [Stoneburner i in. 2002]:

- ocena ryzyka,
- ograniczenie ryzyka,
- monitorowanie i reagowanie na zmiany.

W naszym kraju działalnością standaryzacyjną zajmuje się Polski Komitet Normalizacyjny, w którym utworzono komisje zajmujące się omawianą dziedziną. Ponadto w Polsce funkcjonuje kilka instytucji i organizacji zajmujących się omawianą problematyką. Wśród nich warto zwrócić uwagę na Stowarzyszenie ds. Bezpieczeństwa Systemów Informacyjnych – ISSA Polska, które jest organizacją typu *non profit*, skupiającą profesjonalistów i praktyków zawodowo zajmujących się bezpieczeństwem SI. Celem Stowarzyszenia jest przede wszystkim promowanie zasad i praktyk, które prowadzą do ograniczania ryzyka związanego z bezpieczeństwem systemów informatycznych.

4. Zarządzanie ryzykiem na potrzeby bezpieczeństwa systemów informatycznych według standardów ISO/IEC

Jednym z pierwszych standardów dotyczących bezpieczeństwa SI był dokument opracowany w 1993 roku przez Brytyjski Instytut Normalizacji − BSI (British Standards Institution) i DTI (Department of Trade and Industry), oznaczony symbolem BS PD0003:1993. Wzbudził on na tyle duże zainteresowanie, że skłonił eksper-

tów instytutu do podjęcia prac nad nowym dokumentem, wydanym w 1995 roku – BS 7799 *Code of Practice for Information Security Management*. BS 7799 to norma trzyczęściowa. Jej pierwsza część to kodeks praktyk, zestaw zagadnień, jakie należy realizować dla potrzeb bezpieczeństwa SI. BS 7799-2 to ilustracja, w jaki sposób zaprojektować, wdrożyć i poddać certyfikacji system zarządzania bezpieczeństwem informacji. Trzecia część (BS 7799-3) została opublikowana w 2005 roku i dotyczy zagadnień związanych właśnie z analizą i zarządzaniem ryzykiem na potrzeby bezpieczeństwa SI, również w aspekcie ryzyka biznesowego. Ta część standardu BS przedstawia zagadnienia w zakresie szacowania ryzyka, projektowania i implementacji zabezpieczeń, zarządzania bezpieczeństwem i ponownego szacowania ryzyka.

W roku 2000 zalecenia brytyjskie zawarte we wspomnianej normie zostały poddane normalizacji przez ISO oraz IEC. Wynikiem tych prac była norma ISO/IEC 17799 *Praktyczne zasady zarządzania bezpieczeństwem informacji*. Zastosowanie wytycznych tej normy umożliwia zmniejszenie do minimum ryzyka zafałszowania, a nawet utraty informacji, co na obecnym etapie rozwoju w zakresie technologii informacyjnych jest niemalże koniecznością. Wdrożenie standardu pozwala także określić wymagania przedsiębiorstwa w zakresie bezpieczeństwa, sformułować politykę bezpieczeństwa informacji oraz wybrać odpowiednie środki, dzięki którym jej bezpieczeństwo w organizacji zostanie w wysokim stopniu zapewnione. Norma wspomaga więc procesy organizacyjne w sposób umożliwiający racjonalne podwyższenie bezpieczeństwa systemu, koncentrując się na sferze organizacyjnej oraz kontrolując obszary zwiększonego ryzyka [Jakubowski 2002].

W roku 2005 ukazał się standard ISO 27001 zastępujący normę BS 7799-2, który umożliwia zaprojektowanie i wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) odpowiedniego do potrzeb każdej organizacji. Norma stosuje model „planuj-wykonuj-sprawdzaj-działaj" (PDCA: *Plan-Do-Check-Act*), który przedstawia się następująco [Gapiński, Piłat 2009]:

- Ustanowienie i zarządzanie SZBI – zdefiniowanie polityki określającej ogólny kierunek i zasady działania dotyczące bezpieczeństwa informacji, w tym podejście do szacowania ryzyka. Na tym etapie przeprowadzane są audyty mające na celu identyfikację podatności i ryzyk.
- Wdrożenie i eksploatacja SZBI – na tym etapie organizacja powinna sformułować i wdrożyć plan postępowania z ryzykiem, zaimplementować zabezpieczenia i zdefiniować mierniki ich skuteczności.
- Monitorowanie i przeglądy SZBI – organizacja powinna wykonywać procedury monitorowania i przeglądu, mierzyć skuteczność zabezpieczeń, wykonywać w zaplanowanych odstępach czasu przeglądy ryzyka, przeprowadzać wewnętrzne audyty, przeglądy SZBI, a także uaktualniać plany bezpieczeństwa.
- Udoskonalenie SZBI – organizacja, oprócz operacyjnego zarządzania bezpieczeństwem, zobowiązana jest prowadzić działania związane z ustawicznym doskonaleniem.

W 2008 roku pojawił się międzynarodowy standard traktujący o zarządzaniu ryzykiem bezpieczeństwa informacji ISO/IEC 27005:2008. ISO/IEC 27005 nie zawiera żadnej określonej metodologii zarządzania ryzykiem, jednak standard ten ustanawia i uszczegóławia ramy procesu zarządzania ryzykiem w systemach bezpieczeństwa informacji zgodnych z ISO/IEC 27001. Można zatem skutecznie zarządzać ryzykiem bezpieczeństwa informacji, wykorzystując jedną z wielu istniejących metodologii w tym zakresie, pod warunkiem, że będzie ona spełniać opisane w standardzie wymagania. Wytyczne dla procesu zarządzania ryzykiem zostały opisane w siedmiu rozdziałach tego standardu, który zawiera także sześć dodatkowych załączników, przedstawiających w sposób praktyczny zawarte w normie wytyczne [Abramczyk 2008]. Syntetyczną charakterystykę poszczególnych rozdziałów oraz załączników niniejszego standardu zawarto w tabeli 1.

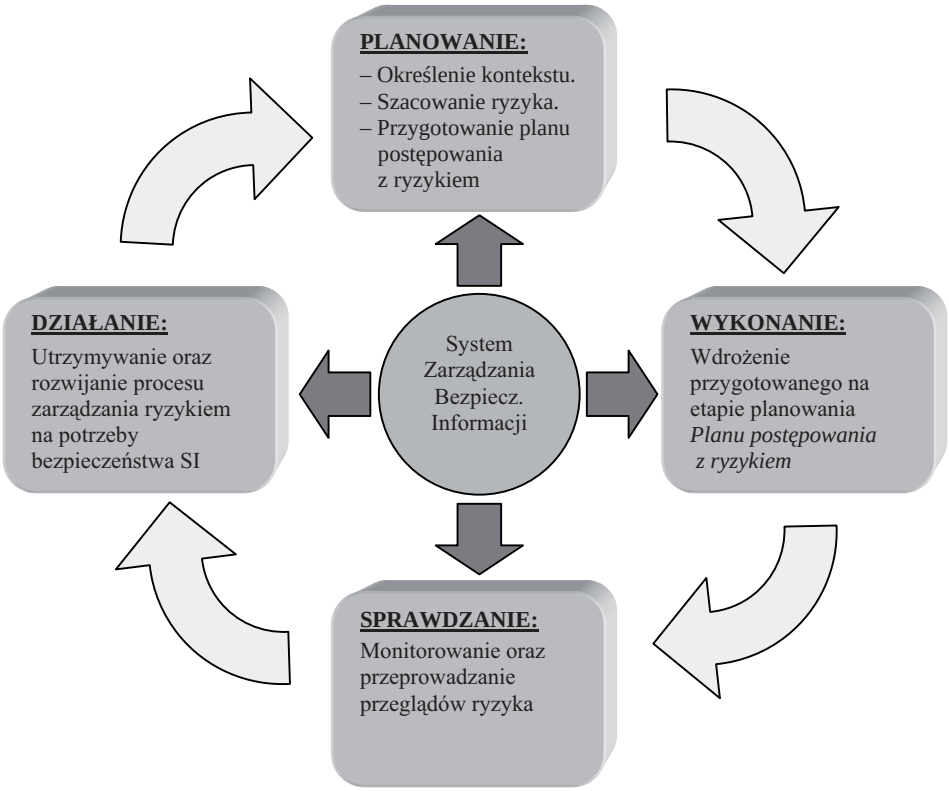
Tabela 1. Charakterystyka standardu zarządzania ryzykiem w systemie bezpieczeństwa informacji ISO/IEC 27005

Rozdział/ załącznik standardu	Nazwa rozdziału/ załącznika standardu	Syntetyczna charakterystyka rozdziału/załącznika standardu
1	2	3
Rozdział 6	*Overview of the information security risk management proces*	Zawiera wytyczne w zakresie procesu zarządzania ryzykiem w systemie bezpieczeństwa informacji. W rozdziale przedstawiono kolejność podejmowania działań i w sposób ogólny opisano poszczególne elementy powtarzającego się procesu zarządzania ryzykiem (tzn. szacowanie, postępowanie i akceptacja ryzyka)
Rozdział 7	*Context establishment*	Zawiera wytyczne dotyczące określenia i ustanowienia warunków procesu zarządzania ryzykiem tzn.: a) podstawowych kryteriów, do których zalicza się: • kryteria oceny ryzyka (uwzględniające m.in. cele strategiczne, wymogi prawa, negatywne konsekwencje na wizerunek i reputację), • kryteria określania wpływu (uwzględniające ważność informacji, utratę atrybutów bezpieczeństwa, straty finansowe, utratę wizerunku, niedotrzymanie terminów umownych), • kryteria akceptacji ryzyka, • określenie zasobów koniecznych do funkcjonowania procesu zarządzania (np. zasady przeprowadzania szacowania ryzyka oraz tworzenia planu postępowania z ryzykiem, środki kontroli oraz monitorowanie i koordynacja procesu zarządzania ryzykiem), b) zakresu i granic procesu zarządzania ryzykiem, c) struktury organizacyjnej ze zdefiniowanymi rolami oraz zakresami obowiązków w obszarze utrzymania i rozwijania procesu zarządzania ryzykiem.

1	*2*	3
Rozdział 8	*Information security risk assessment*	Opisuje wytyczne w zakresie szacowania ryzyka bezpieczeństwa informacji, w tym: • analizę ryzyka (identyfikację aktywów, zagrożeń, zabezpieczeń, podatności, konsekwencji), • ocenę ryzyka.
Rozdział 9	*Information security risk treatment*	• Dostarcza wytycznych w zakresie postępowania z ryzykiem (redakcja, unikanie, transfer ryzyka, akceptacja).
Rozdział 10	*Information security risk acceptance*	• Opisuje wytyczne w zakresie akceptacji ryzyka.
Rozdział 11	*Information security risk communication*	• Określa wytyczne dotyczące informowania zainteresowanych stron na temat ryzyka.
Rozdział 12	*Information security risk monitoring and review*	• Opisuje wytyczne w zakresie monitorowania i przeglądania ryzyka i jego czynników (wartości aktywów, wpływu ryzyka, zagrożeń, podatności, prawdopodobieństwa wystąpienia).
Załącznik A	*Defining the scope and boundaries of information security risk management process*	• Omawia sposób definiowania zakresu oraz granic dla procesu zarządzania ryzykiem na potrzeby bezpieczeństwa informacji. Załącznik ten zawiera wykaz charakterystycznych elementów opisujących organizację w celu przeprowadzenia efektywnej analizy organizacji (A.1), zawiera przykładową listę ograniczeń oddziałujących na organizację (A.2), listę regulacji (zewnętrznych oraz wewnętrznych) mających wpływ na działalność organizacji (A.3) oraz listę ograniczeń oddziałujących na zakres ustanowionego procesu (A.4).
Załącznik B	*Identification and valuation of assets and impact assessment*	• Omawia sposób identyfikacji aktywów (B.1), wyceny aktywów (B.2), szacowania wpływu utraty aktywów i występujących incydentów (B.3).
Załącznik C	*Examples of typical threats*	Zawiera listę przykładowych zagrożeń.
Załącznik D	*Vulnerabilities and methods for vulnerability assessment*	Zawiera zestaw przykładowych podatności oraz metod ich szacowania.
Załącznik E	*Information security risk assessment approaches*	• Zawiera wytyczne w zakresie szacowania ryzyka, tj. ogólne i szczegółowe zasady szacowania ryzyka (np. macierz szacowania ryzyka czy ranking zagrożeń w kontekście wartości ryzyka).
Załącznik F	*Constraints for risk reduction*	• Zawiera informacje dotyczące ograniczeń w zakresie redukcji ryzyka w organizacjach.

Źródło: opracowanie własne na podstawie [Abramczyk 2008].

W odniesieniu do procesów systemu zarządzania bezpieczeństwem informacji (wspomniany model PDCA) elementy zarządzania ryzykiem wpisują się w nie tak jak to przedstawiono na rysunku 1.



Rys. 1. Proces zarządzania ryzykiem a procesy systemu zarządzania bezpieczeństwem informacji w modelu PDCA

Źródło: [Abramczyk 2008]

Norma powyższa dostarcza wiele wytycznych, na podstawie których organizacje mogą opracować i wdrożyć proces zarządzania ryzykiem. Organizacje ISO i IEC są w trakcie opracowywania nowej serii standardów: ISO/IEC 27000; tworzone i dopracowywane są kolejne nowsze normy. Nowa seria standardów, stworzona przez ISO, ma na celu usystematyzowanie wszystkich zaleceń i wymagań dotyczących nie tylko projektowania, budowania i utrzymywania SZBI, ale również zestandaryzowania wymagań co do zarządzania ryzykiem, a w szczególności szacowania ryzyka [*Historia*… 2005].

Czołowy w dziedzinie zarządzania ryzykiem w aspekcie bezpieczeństwa systemów informatycznych w organizacji jest raport techniczny ISO/IEC TR 13335 (*Gu-*

idelines for the Management of IT Security), który składa się z pięciu zasadniczych części. Ich syntetyczną charakterystykę zamieszczono w tabeli 2.

Tabela 2. Syntetyczna charakterystyka standardu ISO/IEC TR 13335

Symbol części raportu	Nazwa części raportu	Syntetyczna charakterystyka części
ISO/IEC TR 13335-1	Wytyczne do zarządzania bezpieczeństwem SI	• terminologia, związki między pojęciami; • podstawowe modele; • trzy podprocesy: zarządzanie ryzykiem, zmianami i konfiguracją;
ISO/IEC TR 13335-2	Technika informatyczna – planowanie i zarządzanie bezpieczeństwem SI	• określenie celów, strategii, polityki bezpieczeństwa; • określenie wymagań w zakresie bezpieczeństwa SI; • różne podejścia do analizy ryzyka; • plany zabezpieczeń – dobór właściwych zabezpieczeń oraz monitorowanie procesu ich wdrażania i funkcjonowania; • organizacja służb odpowiedzialnych za bezpieczeństwo; • znaczenie szkoleń i działań uświadamiających; • role i stanowiska pracy w instytucji związane z bezpieczeństwem; • wykrywanie i reagowanie na incydenty;
ISO/IEC TR 13335-3	Techniki zarządzania bezpieczeństwem systemów informatycznych	• przedstawienie procesów zarządzania; • formułowanie trójpoziomowej polityki bezpieczeństwa; • rozwinięcie problematyki analizy ryzyka i implementacji planu zabezpieczeń; • czynności powdrożeniowe: utrzymanie, monitorowanie i reagowanie na incydenty;
ISO/IEC TR 13335-4	Wybór zabezpieczeń	• klasyfikacja i charakterystyka różnych form zabezpieczeń; • sposoby doboru zabezpieczeń ze względu na rodzaj zagrożenia lub specyfikację systemu; • prezentacja zaleceń wynikających z norm ISO/IEC i innych opracowanych przez różne instytucje; • podejście do analizy ryzyka polegające na wyróżnieniu obszarów wymagających szczegółowej lub podstawowej analizy ryzyka;
ISO/IEC TR 13335-5	Zabezpieczenie dla połączeń z sieciami zewnętrznymi	• dobór zabezpieczeń stosowanych do ochrony styku systemów informatycznych instytucji z sieciami zewnętrznymi.

Źródło: opracowanie własne na podstawie [www.centrumbezpieczenstwa.pl].

W odniesieniu do systemów informatycznych proces zarządzania ryzykiem najpełniej opisany jest w trzeciej części normy *Raport techniczny ISO/IEC TR 13335–3. Technika informatyczna – wytyczne do zarządzania bezpieczeństwem systemów informatycznych*. Dokument zawiera szczegółowe informacje dotyczące trójpoziomowej

polityki bezpieczeństwa. Omówione zostały w nim metody analizy ryzyka, implementacja zabezpieczeń oraz sposobów reagowania na różne incydenty. W raporcie wiele miejsca poświęcono technikom i metodom analizy ryzyka oraz postępowania z nim. Według tego dokumentu punktem wyjścia do efektywnego zarządzania ryzykiem związanym z systemami informatycznymi jest określenie celów instytucji w zakresie bezpieczeństwa SI. W firmie należy opracować strategię bezpieczeństwa informatycznego, która tworzy podstawę polityki bezpieczeństwa instytucji w zakresie systemów informatycznych. Opracowanie polityki bezpieczeństwa jest konieczne w celu zapewnienia, że wyniki procesu zarządzania ryzykiem są właściwe i efektywne [Szczepankiewicz, Szczepankiewicz 2006].

Pierwszym krokiem w procesie zarządzania ryzykiem w obszarze bezpieczeństwa informacji powinno być postawienie pytania: Jaki ogólny poziom ryzyka jest akceptowalny dla instytucji. Kolejny krok to wyznaczenie celów bezpieczeństwa informacyjnego instytucji, podczas którego należy także rozważyć ważne cele biznesowe oraz ich związek z bezpieczeństwem SI. W zależności od celów bezpieczeństwa należy uzgodnić strategię konieczną do osiągnięcia tych celów. Po określeniu strategii bezpieczeństwa i zagadnień wchodzących w jej skład powinna ona stać się podstawą polityki bezpieczeństwa instytucji w zakresie systemów informatycznych i przetwarzanych w nich informacji. Integralnym elementem każdej polityki są procedury, czyli sposoby postępowania, wykonywane w odstępach czasu, mające na celu minimalizowanie czynników ryzyka, które zostały określone w polityce [Szczepankiewicz, Szczepankiewicz 2006].

5. Model referencyjny standardu COBIT a zarządzanie ryzykiem

COBIT (*Control Objectives for Information and Related Technology*) jest zestawieniem dobrych praktyk do zarządzania IT, utworzonych w 1992 roku przez stowarzyszenie ISACA oraz IT Governance Institute. Obecnie obowiązuje czwarta edycja tego pakietu. Metodyka COBIT służy jako pomoc w zarządzaniu, kontroli i audycie systemów informatycznych. W standardzie COBIT 4.1 zarządzanie IT jest analizowane z trzech perspektyw:

- wymagań biznesowych,
- procesów zachodzących w organizacji IT,
- zasobów IT.

COBIT 4.1 dość szczegółowo określa wytyczne w zakresie zarządzania technologiami informatycznymi w organizacji, także w ramach procesów zarządzania i analizy ryzyka informatycznego. W standardzie tym wyróżniono 34 procesy, które zostały podzielone hierarchicznie na trzy części – od ogólnych domen, poprzez procesy, do poszczególnych czynności. Procesy są zgrupowane w 4 podstawowych domenach [Białas 2006, s. 58-59]:

- PO – planowanie i organizacja (ang. *planning and organisation*);
- AI – zakup i wdrożenie (ang. *acquisition and implementation*);

- DS – dostarczanie i wsparcie (ang. *delivery and suport*);
- M – monitorowanie (ang. *monitoring*).

Poszczególne 34 procesy zdefiniowane w standardzie COBIT są związane z zarządzanymi zasobami oraz tak zwanymi wymogami informacyjnymi, stąd symbole P i S (patrz tabela 3) przedstawiają znaczenie danego wymogu dla rozpatrywanego procesu. Każde wymaganie biznesowe jest opisane przez siedem biznesowych wymogów informacyjnych, stanowiących kryteria kontrolne. Są to [www.centrumbezpieczenstwa.pl]:

1) skuteczność (ang. *effectiveness*) – zapewnienie, że informacja w procesach biznesowych jest dla nich odpowiednia i adekwatna, dostarczona na czas w sposób prawidłowy, spójna i użyteczna,

2) wydajność (ang. *efficiency*) – zapewnienie, że dostarczenie informacji odbywa się w ramach optymalnego zużycia zasobów,

3) poufność (ang. *confidentiality*) – zapewnienie, że dostęp do informacji mają tylko osoby uprawnione,

4) integralność (ang. *integrity*) – zapewnienie, że informacja pozostaje dokładna i kompletna,

5) dostępność (ang. *availability*) – zapewnienie, że dostęp do informacji jest możliwy wtedy, gdy jest to wymagane w procesie biznesowym,

6) zgodność (ang. *compliance*) – zapewnienie, że każdy element systemu informacyjnego pozostaje zgodny z przepisami prawa, regulacjami i umowami, dla których przedmiotem jest proces biznesowy,

7) wiarygodność (ang. *reliability*) – zapewnienie właściwych informacji do zarządzania organizacją i dla kierownictwa, aby mogło realizować obowiązki finansowe i sprawozdawcze.

Natomiast wyszczególnione zasoby to ludzie, aplikacje, technologie, urządzenia i dane. Tabela 3 pokazuje procesy standardu COBIT na tle wymogów (kryteriów) informacyjnych i związanych z nimi zasobów. Oznaczone kolorem szarym procesy i wymogi są szczególnie istotne z punktu widzenia problematyki zarządzania ryzykiem w aspekcie bezpieczeństwa informacji w organizacji.

Spośród wyszczególnionych w tabeli 34 procesów informatycznych zdefiniowanych w standardzie COBIT szczególnie interesujący z punktu widzenia tematyki niniejszego artykułu jest proces oznaczony jako PO9, czyli szacowanie ryzyka. W ramach tego procesu zaleca się szacowanie ryzyka do celów biznesowych. Ma ono stanowić wsparcie dla decyzji kierownictwa w zakresie zarządzania ryzykiem. Ryzyko odnosi się w tym przypadku do zagrożeń dla celów strategicznych i operacyjnych poprzez niespełnienie wymogów informacyjnych [Szczepankiewicz, Szczepankiewicz 2006].

W ramach procesu PO9 – szacowanie ryzyka, COBIT definiuje następujące podprocesy [Korytowski 2002; Szczepankiewicz, Szczepankiewicz 2006]:

- PO-9.1. Ocena ryzyka biznesowego
- PO-9.2. Przyjęcie podejścia do oceny ryzyka

Tabela 3. Procesy zarządzania ryzykiem na tle procesu standardu COBIT

Proces	Nazwa	Wymogi							Zasoby				
		1	2	3	4	5	6	7	A	B	C	D	E
PO – Planowanie i organizowanie (ang. *planning and organisation*)													
PO1	Definiowanie planu strategicznego IT	P	S						X	X	X	X	X
PO2	Definiowanie architekt. IT	P	S	S	S					X			X
PO3	Ustalenie kierunku technolog.	P	S								X	X	
PO4	Określenie relacji IT-biznes	P	S						X				
PO5	Zarządzanie inwestycjami IT	P	P					S	X	X	X	X	
PO6	Przedstaw. celów i kierunków rozwoju	P					S		X				
PO7	Zarządzanie zasobami ludzkimi	P	P						X				
PO8	Zapewnienie zgodności z wymog. zewn.	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			
AI – Nabywanie i wdrażanie (ang. *acquisition and implementation*)													
AI1	Identyfikacja zautomatyz. rozwiązań	P	S							X	X	X	
AI2	Nabywanie i utrzymanie oprogramow.	P	P		S		S	S		X			
AI3	Nabywanie i utrzymanie infrastruktury IT	P	P		S						X		
AI4	Rozwijanie i utrzymywanie procedur IT	P	P		S		P	P	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
DS – Dostarczanie i wspieranie (ang. *delivery and support*)													
DS1	Definiowanie poziomów usług	P	P	S	S	S	S	S	X	X	X	X	X
DS2	Zarządzanie usługami zewnętrznymi	P	P	S	S	S	S	S	X	X	X	X	X
DS3	Zarządz. efektywnością i wydajnością	P	P			S				X	X	X	
DS4	Zapewnienie ciągłości usług	P	S			P			X	X	X	X	X
DS5	Zapewnienie bezpieczeństwa SI			P	P	S	S	S	X	X	X	X	X
DS6	Identyfikacja i rozliczanie kosztów		P					P	X	X	X	X	X
DS7	Szkolenie użytkowników	P	S						X				
DS8	Wspomaganie klientów IT	P							X	X			
DS9	Zarządzanie konfiguracją	P				S		S		X	X	X	
DS10	Zarządzanie incydentami	P	P			S			X	X	X	X	X
DS11	Zarządzanie danymi				P			P					X
DS12	Zarządzanie infrastrukturą				P	P						X	
DS13	Zarządzanie operacjami	P	P		S	S			X	X		X	X
M – Monitorowanie (ang. *monitoring*)													
M1	Monitorowanie procesów	P	S	S	S	S	S	S	X	X	X	X	X
M2	Ocena adekwatności kontroli wewnętrz.	P	P	S	S	S	S	S	X	X	X	X	X
M3	Uzyskanie 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

P (ang. *primary*) – pierwszorzędne znaczenie dla oceny procesu przetwarzania informacji, S (ang. *secondary*) – drugorzędne znaczenie dla oceny procesu przetwarzania informacji. Wymogi: 1 – skuteczność, 2 – wydajność, 3 – poufność, 4 – integralność, 5 – dostępność, 6 – zgodność, 7 – wiarygodność. Zasoby: A – ludzie, B – aplikacje, C – technologie, D – urządzenia, E – dane.

Źródło: [Liderman 2008; Białas 2006].

- PO-9.3. Identyfikacja ryzyka
- PO-9.4. Pomiar ryzyka
- PO-9.5. Plan działania w zakresie ryzyka
- PO-9.6. Akceptacja ryzyka
- PO-9.7. Wybór środków bezpieczeństwa
- PO-9.8. Poparcie dla zarządzania ryzykiem

Standard podaje wiele kolejnych wytycznych dotyczących ryzyka i jego szacowania, do których zaliczyć można następujące zalecenia:

- ryzyko informatyczne powinno być regularnie szacowane,
- kierownictwo powinno być powiadamiane o istotnych zmianach w środowisku IT, które mogłyby wpłynąć na scenariusze ryzyka,
- organizacja powinna określić poziom akceptowanego ryzyka i wdrożyć procedury postępowania z ryzykiem nieakceptowanym,
- kierownictwo powinno stale monitorować wielkość ryzyka i w przypadku przekroczenia poziomu ryzyka akceptowanego decydować o jego redukcji, transferze lub innym sposobie postępowania [Szczepankiewicz, Szczepankiewicz 2006].

Standard COBIT może stanowić cenne źródło informacji dla osób odpowiedzialnych za zarządzanie, kontrolę i audyt IT w firmie, w tym również w obszarze zarządzania ryzykiem na potrzeby bezpieczeństwa SI.

6. Zakończenie

Zarządzanie ryzykiem odgrywa obecnie bardzo istotną rolę we wszystkich niemal obszarach funkcjonowania przedsiębiorstw. Należy podkreślić, że korzyści wynikające z właściwego przeprowadzenia procesu zarządzania ryzykiem w organizacji mogą być wielopłaszczyznowe. Istnieje wiele standardów próbujących regulować niniejszą problematykę. Odpowiednie podejście do zarządzania ryzykiem na potrzeby bezpieczeństwa informacji, polegające na wdrożeniu odpowiednich norm, zaleceń, dobrych praktyk, a także implementacji właściwych funkcji, mechanizmów zabezpieczających i kontrolnych, może zmniejszyć znacząco prawdopodobieństwo wystąpienia incydentów, które mogłyby negatywnie wpłynąć na organizację i jej systemy informatyczne. Ich wdrożenie można traktować jako istotny element procesu doskonalenia organizacji pod względem zarządzania bezpieczeństwem systemów informatycznych i przetwarzanych w nich informacji.

Literatura

Abramczyk A., *Zarządzanie ryzykiem w systemie bezpieczeństwa informacji – charakterystyka standardu ISO27005:2008*, http://www.pbsg.pl/index2.php?option=com_content&do_pdf=1&id=445(09.06.2010).

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa 2006.

Gapiński J., Piłat M., *Zarządzanie bezpieczeństwem w banku spółdzielczym*, „Nowoczesny Bank Spółdzielczy" 2009, nr 5.

Historia standardów zarządzania bezpieczeństwem informacji, www.security.dga.pl, Biuletyn Tematyczny „Bezpieczeństwo Informacji" (wrzesień) 2005, nr 1.

ISO/IEC TR 13335-1 *Information Technology − Security Techniques − Guidelines for the Management of IT Security − Part 1: Concepts and Models of IT Security.*

Jakubowski R., *Bezpieczeństwo w standardzie*, ComputerWorld „Bezpieczeństwo danych w sieci" 24.06.2002, http://www.computerworld.pl/artykuly/23677/Bezpieczenstwo.w.standardzie.html (5.10.2010).

Korytowski J., *Praktyki kontrolne w zakresie zarządzania ryzykiem*. Materiały konferencji „Kontrola'02", Bielsko-Biała 2002.

Krupa M., *Ryzyko i niepewność w zarządzaniu formą*, Antykwa, Kraków – Kluczbork 2002.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2008.

Portal internetowy www.centrumbezpieczenstwa.pl (5.10.2010).

Ronka-Chmielowiec (red.), *Zastosowanie metod ekonometryczno-statystycznych w zarządzaniu finansami w zakładach ubezpieczeń*, Wydawnictwo AE we Wrocławiu, Wrocław 2004.

Ronka-Chmielowiec W. (red.), *Zastosowanie metod ilościowych w analizie i ocenie ubezpieczeń dla działalności gospodarczej*, Wydawnictwo UE we Wrocławiu, Wrocław 2009.

Ryba M., *Wielowymiarowa metodyka analizy i zarządzania ryzykiem systemów informatycznych – MIR-2M*, rozprawa doktorska, 2006.

Stoneburner G., Goguen A., Feringa A., *Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Special Publication 800–30*, Washington DC 2002.

Szczepankiewicz E. Szczepankiewicz P., *Zarządzanie ryzykiem informatycznym według międzynarodowych norm i standardów*, „Monitor Rachunkowości i Finansów" 2006, 11.

INSTITUTIONALIZATION AND STANDARDIZATION OF INFORMATION SECURITY RISK MANAGEMENT IN ENTERPRISE

Summary: Modern information systems are often complex, heterogeneous and dynamic. Technological progress and widespread use of information systems in business generate dependencies that cause the increase of diversity, complexity, uncertainty and the amount of risk factors. Therefore risk management, focusing on finding the optimal relationship between the risks and the cost of security issues, becomes increasingly important. Risk cannot be completely avoided, so it must be properly managed. Therefore organizations should implement standards, guidelines and best practices. The article presents selected standards concerning a very rapidly developing area which is information security risk management in an organization. The major ISO/IEC standards and selected best practices in this area are presented.