Ekonomia — Wroclaw Economic Review 24/2 (2018)
Acta Universitatis Wratislaviensis
No 3858

DOI: 10.19195/2084-4093.24.2.8

Agnieszka Krawczyk-Jezierska
ORCID: 0000-0003-1119-0340
Centrum Prawa Bankowego i Informacji
agnieszka.krawczyk@nzb.pl

Jarosław Jezierski
ORCID: 0000-0003-1810-1005
Centrum Prawa Bankowego i Informacji
jaroslaw.jezierski@nzb.pl

Zastosowanie normy ISO/EIC 27001 w sektorze finansowym — zakres i korzyści

Artykuł nadesłany: 14 listopada 2017 r.; **artykuł zaakceptowany:** 20 kwietnia 2018 r.

JEL Classification: G20, G21, L15

Keywords: security, information, standards, finance

Abstract

Application of ISO/EIC 27001 in the financial sector — scope and benefits

In the face of technological advances and, as a result, the increasing threat of the loss of growing amount of data collected by financial institutions, it seems necessary to employ effective security measures in the process of information management. The necessity to implement information security management systems (ISMS) by all institutions processing personal data is reflected in national legislation. The requirements resulting from contemporary hazards and legal provisions are concurrent with the requirements of the international standard ISO/IEC 27001, concerning the designing of the information security management system. This standard is most widely used by IT companies, however, the financial sector that collects and a processes huge amount of personal data, constitutes its significant recipient. Most of the companies certified by this standard come from the Eastern Asia and Pacific region, dominated by Japan, and from Europe, where the United Kingdom is the leader. In Poland the use of ISO/IEC 27001 is growing, yet the financial institutions that fulfill its requirements are still in a minority. It seems that from May 2018 on, national regulations imposing greater responsibility for the security of personal data on the institutions processing it, will bring the above-mentioned standard into focus.

Wstęp

Celem artykułu jest przedstawienie zakresu stosowania normy ISO/IEC (ang. *International Organization for Standarization/International Electrotechnical Commission* — Międzynarodowa Organizacja Standaryzacyjna/Międzynarodowa Komisja Elektrotechniczna) 27001 oraz wynikających z tego korzyści jako odpowiedzi na zagrożenia związane z bezpieczeństwem informacji w sektorze finansowym. Artykuł prezentuje wyniki analizy literatury oraz badań dotyczących zastosowania normy ISO/EIC 27001 w Polsce i na świecie, a także odnoszących się do zagrożeń, na które wskazana norma ma być odpowiedzią, uzupełnione wynikami analizy witryn wybranych polskich instytucji finansowych.

Znaczenie bezpieczeństwa informacji

Informacje gromadzone są na świecie w coraz większej ilości. Według ekspertów branży informatycznej w 2010 roku ludzkość wytwarzała co dwa dni taką ilość danych[1], jaką wytworzyła od swego zarania do 2003 roku[2]. Jednocześnie organizacje, których działania opierają się na gromadzonych w coraz większej ilości informacjach, stają wobec rosnącej skali zagrożeń związanych z globalizacją i postępem technologicznym, skutkujących możliwością utraty swoich zasobów informacyjnych w wyniku różnego rodzaju cyberataków. Raport Światowego Forum Gospodarczego *Global Risks 2015* klasyfikuje takie ryzyka technologiczne, jak kradzieże danych, incydenty związane z cyberbezpieczeństwem oraz awarie infrastruktury w dziesiątce największych zagrożeń dla światowej gospodarki[3]. Według danych z raportu *The Norton Cybercrime Report 2012* na świecie co sekundę 18 osób pada ofiarą cyberprzestępstwa, a każdego dnia jest to 1,5 mln osób. Najwyższy poziom tych przestępstw odnotowuje się w Rosji, Chinach i Afryce Południowej — odpowiednio 92, 84 i 80%[4]. Z kolei zgodnie z raportem PWC Global zatytułowanym *Stan światowego bezpieczeństwa informacji. Przegląd 2017, dane sektorowe: usługi finansowe* (*The Global State of Information Security. Survey 2017, Industry findings: Financial services*) poziom zarejestro-

[1] Autorzy artykułu mają świadomość niespójności definicyjnej pojęć „informacja" i „dane", jednak ze względu na zamienne stosowanie tych terminów w materiałach źródłowych na potrzeby niniejszego artykułu zdecydowali się na traktowanie ich jako synonimów.

[2] Dane podane przez Ericha Schmidta w trakcie „Techonomy Conference" w Lake Tahoe, w Kalifornii (USA), 4 sierpnia 2010 roku — zob. *Google. Erich Schmidt at Techonomy*, https://www.youtube.com/watch?v=UAcCIsrAq70 (dostęp: 30.09.2017).

[3] *Global Risk 2015 10th Edition*, http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf (dostęp: 30.09.2017).

[4] J. Johnson *et al.*, *A comparison of international information security regulations*, „Interdisciplinary Journal of Information, Knowledge, and Management" 9, 2014, s. 89–116, http://www.ijikm.org/Volume9/IJIKMv9p089-116Johnson0798.pdf (dostęp: 30.09.2017).

wanych incydentów wymierzonych przeciwko bezpieczeństwu informacji w instytucjach finansowych raportowany przez respondentów w latach 2013–2016 oscylował wokół 4600−4900 rocznie, aczkolwiek poziom wydatków na bezpieczeństwo informacji wzrósł o 67%, a w roku 2017 — o 11% (w stosunku do roku 2016)[5], co świadczy o zwiększającej się świadomości skutków tego typu ataków i chęci niwelowania ryzyk. Według tego samego raportu 41% respondentów badania uznało ocenę protokołów i norm bezpieczeństwa stron trzecich jako główne wyzwanie w odniesieniu do wysiłków ukierunkowanych na zapewnienie bezpieczeństwa informacji.

Portal branżowy zaufanatrzeciastrona.pl 3 lutego 2017 roku jako pierwszy ujawnił informacje dotyczące cyberataku na polski system finansowy, którego celem — jak się okazało — nie były zasoby finansowe banków, lecz właśnie informacje. Przestępcy komputerowi, potocznie zwani hakerami, po zainfekowaniu serwera Komisji Nadzoru Finansowego spenetrowali systemy informatyczne kilku banków i wykradli dane.

> […] nie mamy jak do tej pory żadnych informacji o powiązanych z tymi atakami udanych lub nieudanych próbach kradzieży środków z rachunków bankowych. Może to wskazywać, że celem atakujących były informacje, a nie pieniądze. W co najmniej jednym przypadku wiadomo, że duże ilości danych zostały przesłane z sieci banku na zewnętrzne serwery […][6].

Według Związku Banków Polskich

> Polski sektor bankowy należy do najlepiej rozwiniętych na świecie. Również stosowane przez polskie banki zabezpieczenia w bankowości internetowej i mobilnej należą do najbardziej zaawansowanych i najnowocześniejszych na świecie, znacznie wyprzedzające technologicznie rozwiązania promowane w Wielkiej Brytanii, Włoszech czy USA[7].

Nie czyni to jednak polskich instytucji finansowych bezpiecznych w 100%. Tym, co skłania organizacje w wielu krajach do wdrażania systemów zarządzania mających na celu ochronę danych wrażliwych, są nie tylko kwestie bezpieczeństwa, lecz także regulacje krajowe. W Polsce według rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[8] wymagania w nim określone uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Nor-

[5] PWC Global, *The Global State of Information Security. Survey 2017, Industry Findings: Financial Services*, https://www.pwc.ru/en/publications/gsiss-2017/financial-services-industry.html (dostęp: 30.09.2017).

[6] https://zaufanatrzeciastrona.pl/post/wlamania-do-kilku-bankow-skutkiem-powaznego-ataku-na-polski-sektor-finansowy/ (dostęp: 30.09.2017).

[7] https://zbp.pl/wydarzenia/archiwum/komentarze/2015/wrzesien/polski-system-finansowy--wyzwania-i-zagrozenia (dostęp: 30.09.2017).

[8] Dz.U. z 2012 r. poz. 526, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20120000526 (dostęp: 30.09.2017).

my PN-ISO/IEC 27001 (czyli polskiego odpowiednika międzynarodowej normy ISO/EIC 27001), a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie innych polskich norm z nią związanych, w tym:

1. PN-ISO/IEC 17799 — w odniesieniu do ustanawiania zabezpieczeń,
2. PN-ISO/IEC 27005 — w odniesieniu do zarządzania ryzykiem,
3. PN-ISO/IEC 24762 — w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

Dzięki temu instytucja może odpierać ewentualne zarzuty o zaniedbania w zakresie bezpieczeństwa informacji za pomocą argumentu o zastosowaniu zaleceń ISO, potwierdzonych przez kompetentne jednostki certyfikacyjne.

Norma ISO 27001

W celu niwelowania zagrożeń względem informacji gromadzonych przez różne rodzaje podmiotów Międzynarodowa Organizacja na Rzecz Normalizacji opracowała serię norm znanych jako ISO 27k, których celem jest pomoc organizacjom w zabezpieczeniu ich aktywów informacyjnych[9]. Za pomocą norm z tej serii organizacja może zarządzać bezpieczeństwem takich aktywów, jak informacje finansowe, własność intelektualna, dane pracownicze lub inne dane powierzone im przez strony trzecie. Rodzina ISO 27000 zawiera kilkadziesiąt norm. Najbardziej znaną z nich jest norma ISO/EIC 27001:2013, która zastąpiła ISO/EIC 27001:2005 i która opisuje wymogi dotyczące Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)[10]. Wywodzi się ona z brytyjskiej normy BS 7799-1 zawierającej wytyczne, które powinny zostać uwzględnione przez firmy przy budowaniu swojego systemu zarządzania bezpieczeństwem informacji, powstałej w 1995 roku jako wynik pracy praktyków z największych brytyjskich firm[11]. Do czerwca 2017 roku polska wersja normy nosiła oznaczenie PN-ISO/IEC 27001:2014-12 i tytuł: *Technika informatyczna — Techniki bezpieczeństwa — Systemy zarządzania bezpieczeństwem informacji — Wymagania.* Norma ta została jednak wycofana i zastąpiona przez PN-EN ISO/IEC 27001:2017-06 (wersja angielska). Aktualizacja polegała na dodaniu oznaczenia „EN". Jest to nadanie normie statusu europejskiego poprzez jej ratyfikację przez jedną z trzech europejskich organizacji normalizacyjnych: Europejski Komitet Normalizacyjny, Europejski Komitet Normalizacji Elektrotechniki lub Europejski Instytut Norm Telekomunikacyjnych. Nowa norma PN-EN ISO/IEC 27001:2017-06 nie zmieniła się pod kątem treści w odniesieniu do normy PN-ISO/IEC 27001:2014-12.

[9] https://www.iso.org/isoiec-27001-information-security.html (dostęp: 30.09.2017); http://www.iso270012013.info/iso27001/family.aspx (dostęp: 30.09.2017).

[10] https://www.iso.org/isoiec-27001-information-security.html (dostęp: 30.09.2017).

[11] M. Borucki, *ISO 27001 — zapewnij bezpieczeństwo informacji*, Warszawa 2013, s. 3.

Stosowanie normy ISO/EIC 27001 na świecie i w Polsce — statystyki

Według *Przeglądu ISO 2016* (*ISO Survey 2016*) w 2016 roku na świecie przyznano 33 290 certyfikatów normy ISO/EIC 27001. Norma ta najbardziej popularna była w krajach południowej Azji i Pacyfiku, a dopiero w drugiej kolejności w Europie i Stanach Zjednoczonych. Liczba tych certyfikatów od 2006 roku systematycznie rośnie. Największy wzrost odnotowano na terenie wschodniej Azji i Pacyfiku oraz w Europie, a najmniejszy w krajach afrykańskich. Prezentuje to tabela 1.

Tabela 1. Liczba certyfikatów normy ISO/IEC 27001 na świecie w podziale na regiony w 2016 roku

Region		Liczba wydanych certyfikatów normy ISO IEC 27001			
		Rok			
		2006	2010	2014	2016
1.	Azja Wschodnia i kraje Pacyfiku	4210	8788	11 303	14 704
2.	Europa	1064	4800	8710	12 532
3.	Azja Środkowa i Południowa	383	1328	2253	2987
4.	Ameryka Północna	79	329	836	1469
5.	Bliski Wschód	37	218	512	810
6.	Ameryka Środkowa i Południowa	18	117	277	564
7.	Afryka	6	46	81	224
8.	Świat	5797	15 626	23 972	33 290

Źródło: opracowanie własne na podstawie *ISO Survey 2016*[12], ISO 27001 — Worldwide Total.

W Polsce w 2016 roku zostało wydanych 657 certyfikatów normy ISO/IEC 27001. Odnotowano także ponad dwukrotny wzrost liczby certyfikatów w stosunku do roku 2014 i prawie sześćdziesięciokrotny w stosunku do 2006. Wzrost liczby certyfikatów w latach 2006–2016 prezentuje tabela 2.

Tabela 2. Liczba certyfikatów normy ISO/IEC 27001 w Polsce

Rok	Liczba certyfikatów
2006	11
2007	45
2008	75
2009	187

[12] http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 (dostęp: 30.09.2017).

2010	229
2011	233
2012	279
2013	307
2014	310
2015	448
2016	657

Źródło: opracowanie własne na podstawie *ISO Survey 2016.*

Liderem regionu wciąż pozostaje Zjednoczone Królestwo, a liderem światowym — Japonia. Polska odnotowuje podobne wartości jak Holandia i Hiszpania. W naszym regionie dwukrotnie więcej certyfikatów mają natomiast Włochy i Niemcy. Dane te zostały zebrane w tabeli 3.

Tabela 3. Liczba certyfikatów normy ISO/IEC 27001 w 10 najlepszych krajach i Polsce w 2016 roku

	Region/kraj	Liczba certyfikatów ISO/EIC 27001:2005
1.	Japonia	8945
2.	Zjednoczone Królestwo	3367
3.	Indie	2902
4.	Chiny	2618
5.	Niemcy	1338
6.	Włochy	1220
7.	USA	1115
8.	Tajwan	1087
9.	Hiszpania	752
10.	Holandia	670
11.	**Polska**	**657**
12.	świat	33 310

Źródło: opracowanie własne na podstawie *ISO Survey 2016.*

W sektorze finansowym w Polsce odnotowano jedynie cztery certyfikacje normy ISO/IEC 27001, nie ma jednak danych o tym, czy wszystkie instytucje finansowe i związane z rynkiem nieruchomości zostały ujęte w badaniu, dane te mogą być więc niepełne.

Sektor finansowy a bezpieczeństwo informacji i norma ISO/IEC 27001

Sektor finansowy z powodu swojej specyfiki polegającej na gromadzeniu, przechowywaniu i przetwarzaniu ogromnej ilości wrażliwych danych oraz prowadzeniu działalności, opierając się na technologiach informatycznych, jest szczególnie narażony na ryzyko związane z utratą zasobów informacyjnych. W sektorze bankowym cyberprzestępstwa stały się bardziej powszechne niż pranie brudnych pieniędzy, oszustwa, przekupstwa czy korupcja[13]. Wraz ze wzrostem powszechności bankowości internetowej rośnie bowiem liczba zagrożeń, do których możemy zaliczyć masowy wyciek danych personalnych w wyniku tak zwanych ataków czy też przypadków DDOS (*distributed denial of service*) — zawieszenia działalności spowodowanej atakiem[14]. W 2016 roku rządy na całym świecie musiały się zmierzyć z masowymi atakami typu DDOS[15]. Liczba osób i mniejszych podmiotów gospodarczych poszkodowanych w tych atakach sięgnęła 83 mln. Podobnie jak w wypadku ataków na polskie instytucje finansowe za pomocą zaatakowanej przez hakerów strony Komisji Nadzoru Finansowego jesienią 2016, o czym była już mowa, w wyniku ataków nie ucierpiały finanse klientów zaatakowanych instytucji finansowych, jednak doszło do utraty danych wrażliwych, takich jak adresy mailowe, adresy zamieszkania i numery telefonów. Inną popularną techniką wykradania danych jest tak zwany ATM skimming[16], który w Stanach Zjednoczonych kosztuje instytucje finansowe setki milionów dolarów rocznie[17].

Problem zagrożeń związanych z bezpieczeństwem informacji dostrzega także branża ubezpieczeniowa. W sierpniu 2016 roku Międzynarodowe Stowarzyszenie Instytucji Nadzoru Ubezpieczeniowego opublikowało raport *Issues Paper on Cyber Risk to the Insurance Sector*, który prezentuje słabości branży oraz zagrożenia związane z zapewnieniem bezpieczeństwa informacji w branży ubezpie-

[13] Stwierdzenie Fazlidy Mohd Razali i Jamaliah Saidy z wystąpienia *Information security: Risk, governance, and implementation setback* na „7th International Conference on Financial Criminology 2015", która odbyła się w dniach 13–14 kwietnia 2015 roku w Wadham College w Oxfordzie, w Wielkiej Brytanii — https://ac.els-cdn.com/S2212567115011065/1-s2.0-S2212567115011065-main.pdf?_tid=39be9cee-a0ac-11e7-a392-00000aab0f01&acdnat=1506204902_8cb8eb10151dac6cb527b9dc62b2b959 (dostęp: 30.09.2017).

[14] P. Youn-Rai, Ch. Yoon-Chul, S. Won-Sung, *Study on financial sector information security level assessment and improvement anticipation model*, „International Journal of Security and Its Applications" 8, 2014, nr 6, s. 147, http://www.sersc.org/journals/IJSIA/vol8_no6_2014/14.pdf (dostęp: 30.09.2017).

[15] *Internet Security Threat Report. Executive Summary*, Symantec, czerwiec 2017, s. 8.

[16] Według *Słownika języka polskiego PWN* jest to „przestępstwo polegające na kopiowaniu pasków magnetycznych i podrabianiu kart płatniczych" — https://sjp.pwn.pl/sjp/skimming;2575576.html (dostęp: 30.09.2017).

[17] G. Zeneli, F. Düsterhöft, *Information Security in Banks and Financial Institutions, Professional Evaluation and Certification Board*, marzec 2016, s. 2, www.pecb.com/article/information-security-in-banks-and-financial-institutions (dostęp: 30.09.2017).

czeniowej. Według raportu efektem ekspozycji na współczesne zagrożenie może być utrata poufnych danych, zakłócenia w prowadzeniu działalności oraz utrata reputacji[18]. Cyberryzyko zajęło czwartą pozycję wśród ryzyk wskazanych przez firmy ubezpieczeniowe w badaniu przeprowadzonym przez PWC oraz Centrum Studiów Innowacji Finansowych[19].

Zapewnienie bezpieczeństwa informacji staje się więc jednym z głównych, o ile nie największym współczesnym wyzwaniem dla instytucji finansowych, które są głównym celem przestępstw w „białych rękawiczkach"[20].

Przedstawiciele kilku znaczących instytucji finansowych w Polsce 13 września 2010 roku dyskutowali na temat zarządzania bezpieczeństwem danych w banku podczas debaty zorganizowanej przez „Miesięcznik Finansowy BANK" w Klubie Bankowca w Warszawie. Uczestnicy zwrócili uwagę, że już w 1997 roku Główny Inspektorat Nadzoru Bankowego pisał o ustanowieniu w bankach systemu zarządzania bezpieczeństwem IT. Zdaniem przedstawicieli sektora po kryzysie finansowym z 2008 roku instytucje finansowe stały się bardziej wyczulone na kwestię niwelowania ryzyk. Od tamtej pory powstały rekomendacje branżowe i krajowe, które są wdrażane przez banki. Za istotny element krajobrazu regulacji i zaleceń związanych z bezpieczeństwem informacji uznano serię norm ISO 27k jako niewymieniające konkretnych działań, lecz identyfikujące obszary zagrożeń i wskazujące, „co" należy zrobić, a nie „jak" to zrobić[21].

W grudniu 2014 roku Europejska Agencja Bezpieczeństwa Sieci i Informacji ENISA opublikowała raport *Bezpieczeństwo sieci i informacji w sektorze finansowym. Krajobraz regulacyjny i priorytety sektora*, do którego przebadała instytucje nadzorcze i finansowe z 28 krajów członkowskich Unii Europejskiej. Raport zwraca uwagę na normy zarówno krajowe, jak i sektorowe oraz rozwiązania europejskie, a także na wysokie koszty zgodności (*compliance*) dla instytucji finansowych działających w różnych krajach i podlegających odmiennym regulacjom. Dlatego też wiele instytucji, które wzięły udział w badaniu, wskazało na między-

[18] International Association of Insurance Supervisors, *Issues Paper on Cyber Risk to the Insurance Sector*, s. 9–10, https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector (dostęp 30.09.2017)

[19] PWC Global, Centre for the Study of Financial Innovation, *Insurance Banana Skins 2015: The CSFI Survey of the Risks Facing Insurers*, lipiec 2015, akapit 1, http://static1.squarespace.com/static/54d620fce4b049bf4cd5be9b/t/55dde0fce4b0dff05004146c/1440604412304/2015+Insurance+Banana+Skins+FINAL.pdf (dostęp: 30.09.2017).

[20] R.L. Price, J.S. Cotner, W.L. Dickson, *Computer fraud in commercial banks: Management's perception*, „Journal of Systems Management" 1989, 40 (10), s. 28, cyt. za: K. Streff, *An Information Security Management System Model for Small and Medium-sized Financial Institutions*, s. 1, https://www.researchgate.net/publication/228991064_AN_INFORMATION_SECURITY_MANAGEMENT_SYSTEM_MODEL_FOR_SMALL_AND_MEDIUM-SIZED_FINANCIAL_INSTITUTIONS (dostęp: 30.09.2017).

[21] M. Kozak, *Zarządzanie bezpieczeństwem danych w banku*, „Miesięcznik Finansowy BANK" październik 2010, https://alebank.pl/zarzdzanie-bezpieczestwem/?id=6407&catid=372 (dostęp: 30.09.2017).

narodowe standardy nienormatywne, takie jak ISO/IEC 27001 oraz normę branżową PCI Data Security Standard (PCI DSS) stworzoną przez grupę organizacji płatniczych (między innymi American Express, Discover Financial Services, JCB i MasterCard and Visa International) jako możliwość niwelowania różnic legislacyjnych w zakresie zapewnienia bezpieczeństwa sieci i informacji[22].

Certyfikowanie normą ISO/IEC 27001 w sektorze finansowym

Zgodnie z cytowanym *Przeglądem ISO 2016* w części prezentującej certyfikaty normy ISO/IEC 27001 w podziale na sektory, w sektorze o numerze 32 pod nazwą „Pośrednictwo finansowe, rynek nieruchomości, wynajem" liczba certyfikatów w 2006 roku wynosiła 47, a w 2016 zanotowała wzrost do wartości 250. Jednocześnie w sekcji 33 „Technologia informacyjna" liczby te wynoszą odpowiednio 890 i 6578, co daje temu sektorowi miejsce w czołówce. Pośrednictwo finansowe, nieruchomości i wynajem znajduje się bowiem w pierwszej piątce sektorów o największej liczbie wydanych certyfikatów ISO/IEC 27001 i plasuje się za następującymi sektorami:

1. „Technologie informacyjne",
2. „Inne usługi",
3. „Transport, przechowywanie, komunikacja",
4. „Sprzęt elektryczny i optyczny"[23].

Sektor ten na piątym miejscu zastąpił „Zdrowie i działania społeczne", które uplasowały się na tej pozycji w 2015 roku.

Liczby certyfikatów wydanych w sektorze finansowym, który w raporcie określony jest jako „Pośrednictwo finansowe, nieruchomości i wynajem", w wybranych krajach naszego regionu i świata zostały przedstawione w tabeli 4.

Tabela 4. Liczba wydanych certyfikatów normy ISO/IEC 27001 w 2016 r. w sektorze Pośrednictwo finansowe, nieruchomości, wynajem

Lp.	Kraj	Liczba wydanych certyfikatów normy ISO/IEC 27001 w 2016 roku w sektorze „Pośrednictwo finansowe, nieruchomości, wynajem"
1.	Japonia	44
2.	Zjednoczone Królestwo	16
3.	Izrael	10

[22] European Union Agency for Network and Information Security, *Network and Information Security in the Finance, Regulatory Landscape and Industry Priorities Sector*, https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector (dostęp: 30.09.2017).

[23] Na podstawie *ISO Survey 2016: Certificates by industrial sector. Top five industrial sectors for ISO/IEC 27001 certificates 2016*.

4.	Niemcy	10
5.	Włochy	10
6.	Węgry	8
7.	**Polska**	**4**
8.	Hiszpania	4
9.	Francja	3
10.	Litwa	2
11.	Słowacja	2
12.	Słowenia	2
13.	Republika Czeska	1
14.	Estonia	0
15.	Łotwa	0
16.	Stany Zjednoczone	0

Źródło: opracowanie własne na podstawie *ISO Survey 2016*.

Na podstawie raportu można stwierdzić, że polski sektor finansowy nie odbiega w liczbie certyfikacji od innych krajów naszego regionu. Należy jednak zaznaczyć, że nie wszyscy respondenci raportu udostępnili dane, o czym była już mowa. Według danych portalu soscertyfikacja.pl prowadzącego rejestr certyfikatów norm ISO wydanych w Polsce, który prezentuje 67 instytucji posiadających certyfikaty normy ISO/IEC 27001, a więc również jest rejestrem niepełnym, odnotowano 13 certyfikacji w sektorze finansowym[24].

Instytucje finansowe w Polsce zaczynają dostrzegać korzyści wynikające z wdrożenia normy ISO/IEC 27001. Pierwszym bankiem w Polsce, który wdrożył te zalecenia już w 2008 roku, był Bank Spółdzielczy w Wysokiem Mazowieckiem[25], który jednocześnie zamieścił na swojej witrynie Politykę Zarządzania Systemem Bezpieczeństwem Informacji i udostępnił ją klientom i partnerom biznesowym. Wśród banków komercyjnych działających w Polsce posiadanie certyfikatu deklarują takie duże banki, jak Bank Zachodni WBK S.A., PKO Bank Polski S.A., BGŻ BNP Paribas S.A. i City Handlowy[26] oraz takie instytucje finansowe, jak Biuro Informacji Kredytowej, Krajowa Izba Rozliczeniowa i Biuro Informacji Gospodarczej Krajowy Rejestr Długów, Kasa Rolniczego Ubezpieczenia Społecznego, Inteligo Financial Services S.A., LeasePlan Fleet Management

[24] http://www.soscertyfikacja.pl/jednostki-kategorie/iso-27001-lista-wydanych-certyfikatow/page/2/ (dostęp: 30.09.2017).

[25] https://www.bswysokiemazowieckie.pl/o-banku/nagrody-i-wyr%C3%B3%C5%BCnienia.html (dostęp: 30.09.2017).

[26] Przeanalizowano strony internetowe 49 banków komercyjnych zrzeszonych w Związku Banków Polskich — https://zbp.pl/czlonkowie/lista-bankow (dostęp: 30.09.2017).

(Polska) Sp. z o.o., Europejskie Konsorcjum Ubezpieczeniowe Sp. z o.o., Energo-Invest-Broker S.A. oraz Atlantic Fund Services Sp. z o.o.[27]

Niektóre banki nie wdrażają normy ISO/IEC 27001, jednak deklarują postępowanie zgodne z zaleceniami normy. W raporcie *CSR 2014* Banku Millennium czytamy:

> System zarządzania bezpieczeństwem informacji stosowany w Banku wzorowany jest na międzynarodowej normie ISO/IEC 27001, w której określono wymagania dotyczące ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia zarządzania bezpieczeństwem informacji w organizacji. Przegląd regulacji dotyczących zarządzania bezpieczeństwem informacji dokonywany jest przynajmniej raz w roku. Przyjęty model zarządzania bezpieczeństwem informacji wyznacza kompleksowy system ochrony wszelkich informacji przetwarzanych w Banku, w tym dotyczących zarówno Klientów, Pracowników oraz realizowanych transakcji[28].

Zapis sugeruje, że pomimo braku certyfikacji bank stosuje się do zasad opisanych w omawianej normie i zapewnia bezpieczeństwo informacji według zawartych w niej zapisów.

Korzyści wynikające z wdrożenia normy ISO/IEC 27001 w instytucji finansowej

Instytucje finansowe jak każde inne muszą chronić informacje o swoich klientach, które tworzą, przetwarzają czy też przechowują. Dane, w szczególności dotyczące finansów osobistych (zobowiązania, kredyty, oszczędności, wpływy na konto itp.), należą do bardzo istotnych dóbr osobistych człowieka. Powinny więc być chronione przed udostępnianiem osobom nieupoważnionym, nieautoryzowaną zmianą, zniszczeniem, utratą czy uszkodzeniem[29]. Coraz większa liczba firm oczekuje twardych dowodów zapewnienia jakości przez swoich kontrahentów w zakresie bezpieczeństwa informacji.

Równolegle do kwestii dotyczących satysfakcji klientów pojawiają się również pytania o bezpieczeństwo procesów związanych z ochroną przekazanych informacji. Ma to szczególne znaczenie, gdy przedsiębiorstwo przekazuje drugiemu wiele swoich poufnych informacji. Ze szczególnym przypadkiem takiego powierzania danych mamy do czynienia w momencie współpracy bank–firma, na przykład podczas udzielania kredytu. W trakcie rozpatrywania wniosku kredytowego analitycy bankowi mają wgląd do wielu ważnych dokumentów, takich jak sprawozdania finansowe, biznesplany, kontrakty itp. Z tego względu wiele

[27] http://www.soscertyfikacja.pl/jednostki-kategorie/iso-27001-lista-wydanych-certyfikatow/page/2/ (dostęp: 30.09.2017).

[28] http://raportcsr.bankmillennium.pl/cgiutils/001_Zapewnienie%20bezpieczenstwa%20powierzonych%20srodkow%20%20Millennium%20Raport%20CSR%202014.pdfb31d.pdf (dostęp: 30.09.2017).

[29] https://www.bik.pl/bezpieczenstwo-danych (dostęp: 30.09.2017).

instytucji finansowych decyduje się na wdrożenie SZBI lub chociażby deklaruje stosowanie zaleceń w nich zawartych.

Korzyści z wdrożenia SZBI i ochrony informacji można podzielić na pięć kategorii:

1. biznesowe,
2. wewnętrzne,
3. zewnętrzne,
4. dla klientów i innych stron trzecich,
5. marketingowe[30].

Najważniejszą kwestią dla przedsiębiorstwa jest zapewnienie ciągłości biznesu, a także ograniczenie strat poprzez unikanie przede wszystkim przecieków poufnych i strategicznych informacji do konkurencji lub mediów. Zabezpieczenie informacji na wypadek katastrof i awarii umożliwia ciągłość prowadzenia biznesu, co automatycznie przekłada się na uniknięcie bądź zmniejszenie strat finansowych.

Korzyści z wdrożenia SZBI może być wiele — dla każdego przedsiębiorstwa mogą być one różne i nie zawsze te same. Może to być między innymi:

— wprowadzenie i utrzymanie w mocy działań i form zachowań, będących wyrazem poczucia odpowiedzialności za sprawy związane z bezpieczeństwem informacji;

— zredukowanie poziomu ryzyka związanego z utratą kontroli nad bezpieczeństwem informacji;

— korzyści marketingowe — budowanie przewagi konkurencyjnej poprzez poprawę wizerunku i ochronę marki, a ostatecznie zwiększenie zaufania klientów;

— zwiększenie wiarygodności przedsiębiorstwa poprzez wdrożenie certyfikatu w opinii klientów, kontrahentów;

— ułatwienia w integracji systemów w wypadku łączenia banków polskich i zagranicznych;

— korzyści dla klientów — zapewnienie ochrony informacji;

— spełnienie wymogów dotyczących bezpieczeństwa informacji określonych w regulacjach europejskich i krajowych[31].

Jak wynika z badań przeprowadzonych w sektorze małych i średnich przedsiębiorstw[32], 47% ankietowanych wiąże utratę poufnych danych z konkretnymi stratami finansowymi, 28% do negatywnych konsekwencji wycieku informacji zalicza brak zaufania klientów i kontrahentów, a 25% — utratę reputacji lub dobrego wizerunku firmy. Autorzy artykułu stwierdzają, że w świetle zrealizowanych badań „informacje stanowią jedną z najwyżej cenionych wartości w bizne-

[30] J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji*, Poznań 2009, s. 32.

[31] *Ibidem*, s. 31.

[32] M. Pałęga, M. Knapiński, W. Kulma, *Ocena systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie w świetle przeprowadzonych badań*, Opole 2014, s. 419–426.

sie" oraz że „świadomość organizacji (kierowników i pracowników) w zakresie uznawania informacji i jej bezpieczeństwa za priorytet w prowadzonej działalności gospodarczej będzie systematycznie wzrastać"[33].

Podsumowanie

Rozporządzenie ogólne o ochronie danych osobowych (RODO) zaczęło obowiązywać 25 maja 2018 roku[34]. Dotyczy ono wszystkich firm (nie tylko finansowych), które gromadzą dane osób fizycznych. Jednak — jak pokazują analizy firmy DELL[35] — 97% badanych firm nie miało przygotowanych planów do spełnienia wymogów wskazanego rozporządzenia na pół roku przed datą rozpoczęcia jego obowiązywania. Trzy miesiące później raport PWC potwierdził, że wciąż niegotowych na RODO było 97% polskich firm[36]. Wdrożenie przez instytucje finansowe Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymogami Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych lub z normą ISO/IEC 27001 — gdyż rozporządzenie uznaje wypełnienie wymogów normy jako spełnienie wymogów rozporządzenia — może być pomocne w kontekście RODO, gdyż norma międzynarodowa ISO/IEC 27001 ma szerszy zakres i dotyczy zarządzania bezpieczeństwem informacji, których częścią są dane osobowe.

Bibliografia

Źródła

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz. UE OJ L 119 z 4.05.2016, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A32016R0679.

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. z 2012 r. poz. 526, http://isap.sejm.gov.pl/DetailsServlet?id=WDU20120000526.

[33] *Ibidem*, s. 421.

[34] Rozporządzenie Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz.Urz. UE OJ L 119 z 4.05.2016.

[35] https://odoserwis.pl/a/1069/badanie-firmy-dell-przedsiebiorstwa-nie-sa-gotowe-na-unijne-rozporzadzenie-o-ochronie-danych-gdpr (dostęp: 30.09.2017).

[36] *Cyber-ruletka po polsku. 5. edycja Badania Stanu Bezpieczeństwa Informacji*, https://www.pwc.pl/badaniebezpieczenstwa (dostęp: 10.07.2018).

Literatura

Borucki M., *ISO 27001 — zapewnij bezpieczeństwo informacji*, Warszawa 2013.
Internet Security Threat Report. Executive Summary, Symantec, czerwiec 2017.
Johnson J., Lincke S.J., Imhof R., Lim C., *A comparison of international information security regulations*, „Interdisciplinary Journal of Information, Knowledge, and Management" 9, 2014, http://www.ijikm.org/Volume9/IJIKMv9p089-116Johnson0798.pdf.
Kozak M., *Zarządzanie bezpieczeństwem danych w banku*, „Miesięcznik Finansowy BANK" październik 2010, https://alebank.pl/zarzdzanie-bezpieczestwem/?id=6407&catid=372.
Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji*, Poznań 2009.
Mohd Razali F., Said J., *Information security: Risk, governance and implementation setback*, „Procedia Economics and Finance" 28, 2015, https://www.sciencedirect.com/science/article/pii/S2212567115011065.
Pałęga M., Knapiński M., Kulma W., *Ocena systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie w świetle przeprowadzonych badań*, Opole 2014.
Price R.L., Cotner J.S., Dickson W.L., *Computer fraud in commercial banks: management's perception*, „Journal of Systems Management" 1989, 40 (10).
PWC Global, *The Global State of Information Security. Survey 2017, Industry Findings: Financial Services*, https://www.pwc.ru/en/publications/gsiss-2017/financial-services-industry.html.
PWC Global, Centre for the Study of Financial Innovation, *Insurance Banana Skins 2015. The CSFI Survey of the Risks Facing Insurers*, lipiec 2015, http://static1.squarespace.com/static/54d620fce4b049bf4cd5be9b/t/55dde0fce4b0dff05004146c/1440604412304/2015+Insurance+Banana+Skins+FINAL.pdf.
Streff K., *An Information Security Management System Model for Small and Medium-sized Financial Institutions*, https://www.researchgate.net/publication/228991064_AN_INFORMATION_SECURITY_MANAGEMENT_SYSTEM_MODEL_FOR_SMALL_AND_MEDIUM-SIZED_FINANCIAL_INSTITUTIONS.
Youn-Rai P., Yoon-Chul Ch., Won-Sung S., *Study on financial sector information security level assessment and improvement anticipation model*, „International Journal of Security and Its Applications" 8, 2014, nr 6, http://www.sersc.org/journals/IJSIA/vol8_no6_2014/14.pdf.
Zeneli G., Düsterhöft F., *Information Security in Banks and Financial Institutions, Professional Evaluation and Certification Board*, marzec 2016, www.pecb.com/article/information-security-in-banks-and-financial-institutions.

Źródła internetowe

Cyber-ruletka po polsku. 5. edycja Badania Stanu Bezpieczeństwa Informacji, https://www.pwc.pl/badaniebezpieczenstwa.
European Union Agency for Network and Information Security, *Network and Information Security in the Finance, Regulatory Landscape and Industry Priorities Sector*, https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector.
International Association of Insurance Supervisors, *Issues Paper on Cyber Risk to the Insurance Sector*, https://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector.
Global Risk 2015 10th Edition, http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf.
Google. Erich Schmidt at Techonomy, https://www.youtube.com/watch?v=UAcCIsrAq70.
http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1.
http://raportcsr.bankmillennium.pl/cgiutils/001_Zapewnienie%20bezpieczenstwa%20powierzonych%20srodkow%20%20Millennium%20Raport%20CSR%202014.pdfb31d.pdf.
http://sklep.pkn.pl/pn-iso-iec-27001-2014-12p.html.
http://www.iso270012013.info/iso27001/family.aspx.

http://www.pkn.pl/sites/default/files/w10_2015.pdf.
http://www.soscertyfikacja.pl/jednostki-kategorie/iso-27001-lista-wydanych-certyfikatow/page/2/.
https://ac.els-cdn.com/S2212567115011065/1-s2.0-S2212567115011065-main.pdf?_tid=39be9cee-a0ac-11e7-a392-00000aab0f01&acdnat=1506204902_8cb8eb10151dac6cb527b9dc62b2b959.
https://odoserwis.pl/a/1069/badanie-firmy-dell-przedsiebiorstwa-nie-sa-gotowe-na-unijne-rozporzadzenie-o-ochronie-danych-gdpr.
https://sjp.pwn.pl/sjp/skimming;2575576.html.
https://www.bik.pl/bezpieczenstwo-danych.
https://www.bswysokiemazowieckie.pl/o-banku/nagrody-i-wyr%C3%B3%C5%BCnienia.html.
https://www.iso.org/isoiec-27001-information-security.html.
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.
https://zaufanatrzeciastrona.pl/post/wlamania-do-kilku-bankow-skutkiem-powaznego-ataku-na-polski-sektor-finansowy/.
https://zbp.pl/czlonkowie/lista-bankow.
https://zbp.pl/wydarzenia/archiwum/komentarze/2015/wrzesien/polski-system-finansowy-wyzwania-i-zagrozenia.