# AUDYT ZGODNOŚCI Z NORMĄ ISO/IEC 27001:2013, JAKO NARZĘDZIE DIAGNOZY I DOSKONALENIA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W PRZEDSIĘBIORSTWIE

**Michał PAŁĘGA, Marcin KNAPIŃSKI**

**Streszczenie:** W artykule przedstawiono audyt zgodności systemu zarządzania bezpieczeństwem informacji (SZBI) z normą ISO/IEC 27001:2013, jako narzędzie diagnostyczne i doskonalące stan bezpieczeństwa w przedsiębiorstwie. W poszczególnych podrozdział publikacji przybliżono normę ISO/IEC 27001:2013, omówiono pojęcie i rodzaje audytu, a także przedstawiono niezbędne działania, jakie składają się na proces audytowy. Obok rozważań teoretycznych zaprezentowano również studium przypadku (case study) dotyczące audytu SZBI, z uwypukleniem przykładowych niezgodności SZBI z normą ISO/IEC 27001. Dla podkreślenia znacznych walorów audytu wskazano potencjalne działania korygujące oraz obszary wymagające doskonalenia.

**Słowa kluczowe:** audyt, audyt wewnętrzny, bezpieczeństwo informacji, system zarządzania bezpieczeństwem informacji SZBI.

## 1. Wstęp

Współcześnie informacje stanowią strategiczne aktywa każdej instytucji oraz jednostki gospodarczej, wpływając na ich istnienie na rynku oraz determinując sukces w prowadzaniu działalności biznesowej i utrzymanie konkurencyjności. Zasoby informacyjne powszechnie uznaje się za towar, który obok dóbr materialnych czy energii posiada określoną wartość i podlega wymianie rynkowej. Zgodnie z normą ISO/IEC 27001:2013 informacje są aktywem, który podobnie jak inne aktywa biznesowe, są cenne dla biznesu i wymagają ochrony przed zagrożeniami [8]. Szczególne znaczenie ochrony informacji wynika z faktu, że są one przetwarzane i transmitowane za pomocą rozmaitych narzędzi i technologii informatycznych, co powoduje większą różnorodność zagrożeń, pochodzącą z wielu źródeł [12].

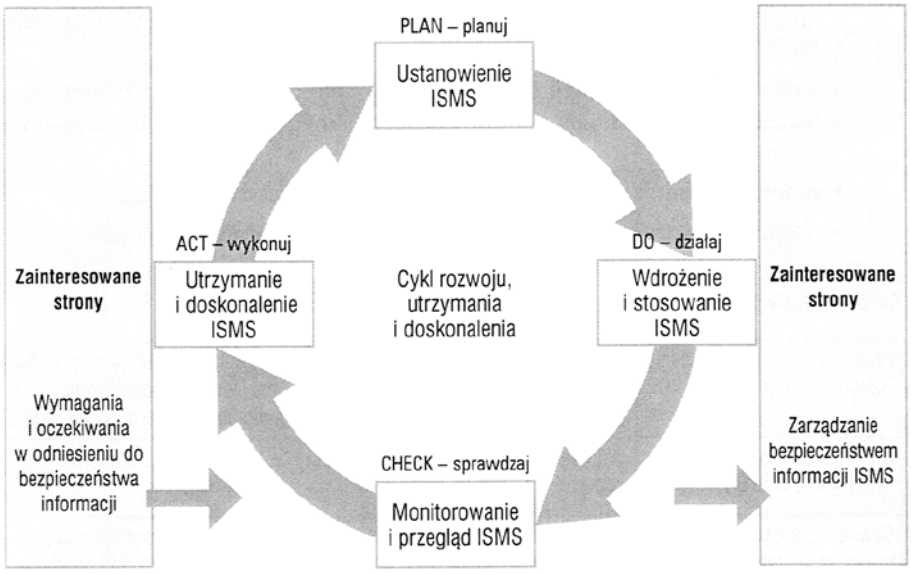
Podstawowym problemem związanym z zarządzaniem bezpieczeństwem informacji jest ich wielopostaciowość. Informacje mogą przybierać zarówno formę pisaną, drukowaną, jak i mówioną (słowo mówione). Poza tym mogą one być przechowywane w systemach komputerowych (np. serwery plików, komputery, urządzania mobilne, bazy danych, aplikacje) oraz w postaci dokumentów papierowych. Oprócz tego wskazać należy na różne środki jej przesyłania i udostępniania: poczta, fax, urządzania elektroniczne i audiowizualne. Szczególną formę informacji stanowią wiedza i umiejętności każdego pracownika organizacji. Jednakże bez względu na formę występowania oraz środki udostępniania i utrwalania informacji wymagają one zawsze właściwej ochrony [12]. Stąd też przedsiębiorstwa zobligowane są do budowania, utrzymania oraz doskonalenia własnego systemu zarządzania bezpieczeństwa informacji, który oparty może być o rozwiązania zaproponowane w międzynarodowym standardzie ISO/IEC 27001:2013.

Podstawą do zapewnienia właściwego funkcjonowania tego systemu jest przeprowadzanie audytu, który pozwala zidentyfikować występujące niezgodności i problemy, a także podjąć skuteczne działania zapobiegawcze i doskonalące.

## 2. System zarządzania bezpieczeństwem informacji wg normy ISO/IEC 27001:2013

ISO/IEC 27001:2013 to międzynarodowa norma, która standaryzuje system zarządzania bezpieczeństwa informacji (SZBI). Wskazuje ona, jak należy właściwie zaprojektować system zarządzania bezpieczeństwem informacji oraz jak go utrzymać i adaptować do zmieniających się warunków otoczenia jednostki gospodarczej. Norma ta zawiera wymagania w zakresie ustanawiania, wdrażania, eksploatacji, monitorowania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji.

W modelu SZBI opisanym w normie ISO/IEC 27001:2013 zastosowano podejście procesowe oparte na cyklu PDCA (ang. Plan – Do – Check – Act), co przestawia rys. 1. Ważnym odnotowania jest fakt, że zastosowanie modelu PDCA nie zostało przywołane wprost jako wymaganie do zastosowania, a więc dopuszcza się wybór innego podejścia.




Rys. 1. Model PDCA stosowany w procesach SZBI
Źródło: [12]

W modelu PDCA wyróżniono cztery podstawowe fazy, do których należą [4, 6, 12]:
**Faza planowania** *(ang. Plan)* – koncentruje się ona na ustanowieniu SZBI oraz celów, procedur i procesów znaczących dla zarządzania ryzykiem, szacowania ryzyka, jak również doskonalenia bezpieczeństwa informacji w organizacji.
**Faza działania** *(ang. Do)* – polega na implementacji i eksploatacji polityki SZBI, zabezpieczeń, procesów i procedur.
**Faza sprawdzania** *(ang. Check)* – obejmuje monitorowanie i przegląd SZBI, szacowanie, pomiar wydajności procesów w odniesieniu do polityki SZBI oraz dostarczanie

kierownictwu raportów do przeglądu.

**Faza wykonywania** *(ang. Act)* – to utrzymanie i doskonalenie SZBI, co wymaga podejmowania działań korygujących i zapobiegawczych w oparciu o audyt SZBI, przegląd dokonywany przez kierownictwo organizacji oraz inne istotne informacje, w celu zagwarantowania ciągłego doskonalenia SZBI.

System zarządzania bezpieczeństwem informacji oparty na normie ISO/IEC 27001:2013 charakteryzuje także kompleksowe zastosowanie, bowiem pozwala ona na wybór zabezpieczeń w czterech podstawowych obszarach: fizycznym, osobowym, teleinformatycznym oraz prawnym. Norma w sposób konkretny nie precyzuje, jakiego rodzaju środki ochronne powinny zostać wdrożone w organizacji, lecz wskazuje obszary wymagające uregulowania. Zakłada ona, że wybór określonych mechanizmów zabezpieczających powinien być kwestią indywidualną każdego przedsiębiorstwa, odpowiadającą potrzebom zdefiniowanym w procesie analizy ryzyka, a także wynikać m.in. z wielkości organizacji, rodzaju realizowanych procesów biznesowych czy zasobów finansowych.

W załączniku A analizowanej normy wyszczególniono 14 obszarów, determinujących bezpieczeństwo informacji w organizacji. Należą do nich [8]:

1. Polityka bezpieczeństwa informacji
2. Organizacja bezpieczeństwa informacji
3. Bezpieczeństwo zasobów ludzkich
4. Zarządzanie aktywami
5. Kontrola dostępu
6. Kryptografia
7. Bezpieczeństwo fizyczne i środowiskowe
8. Bezpieczna eksploatacja
9. Bezpieczeństwo komunikacji
10. Pozyskiwanie, rozwój i utrzymanie systemów
11. Relacje z dostawcami
12. Zarządzanie incydentami związanymi z bezpieczeństwem informacji
13. Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
14. Zgodność

System zarządzania bezpieczeństwem informacji zgodny z normą ISO/IEC 27001:2013 ze względu na swoje kompleksowe podejście charakteryzuje się także uniwersalnością zastosowania i może zostać wdrożone w różnego rodzaju organizacjach, takich jak: banki, jednostki administracji publicznej, jednostki służby zdrowia, a także organizacje non – profit.

## 3. Istota audytu i jego rodzaje

Pojęcia audytu w sposób najbardziej ogólny definiuje norma ISO 19001:2012 zgodnie z którą audyt to systematyczny, niezależny i udokumentowany proces uzyskania dowodów z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu [7].

Przytoczona definicja audytu oprócz tego, iż wskazuje na trzy zasadnicze cechy audytu, dotyczy także procesu audytowego, który powinien zostać udokumentowany oraz przeprowadzony zgodnie z ustalonymi kryteriami audytu [11]. *Kryteria audytu* obejmują zestaw polityk, procedur i wymagań stanowiących odniesienie do audytu. Z kolei przez

*dowód z audytu* należy rozumieć zapis, stwierdzenie faktu lub inne możliwe do zweryfikowania informacje istotne za względu na kryteria audytu [2, 4, 6, 10].

Podkreślić należy także to, iż *audyt nie jest kontrolą*, a jego celem nie jest poszukiwanie niezgodności i osób za nie odpowiedzialnych [1].

Wyróżnia się trzy zasadnicze rodzaje audytu SZBI, do których zalicza się: [1]

- audyt pierwszej strony (wewnętrzny) – przeprowadzany przez pracowników danego przedsiębiorstwa w celu weryfikacji poszczególnych elementów SZBI pod kątem ich skuteczności i zgodności z normą ISO/IEC 27001:2013;
- audyt drugiej strony (zewnętrzny) – przeprowadzany przez pracowników przedsiębiorstwa audytującego; jego celem jest przede wszystkim nadzór na skutecznością SZBI, jaki funkcjonuje u dostawców (podwykonawców);
- audyt trzeciej strony (certyfikujący) – przeprowadzany przez zespół audytorów niezależnych jednostek certyfikujących, wykonywany obowiązkowo przed rozpoczęciem procedury certyfikacji SZBI.

Audyt stanowi szczególnie cenne narzędzie, z którego można korzystać zarówno na etapie wdrażania systemu zarządzania, jaki i jego eksploatacji i ciągłego doskonalenia. Audyt bowiem umożliwia potwierdzenie zgodności rozwiązań, wskazanie słabych miejsc i punktów systemu (niezgodności) oraz analizę przyczyn ich powstawania i skutków, a także podejmowanie działań naprawczych i profilaktycznych [3, 4]. Podczas przeprowadzania audytu SZBI zespół audytorski dokonuje weryfikacji zgodności systemu lub jego poszczególnych elementów z wymaganiami normy ISO/IEC 27001:2013, regulacjami prawnymi oraz innymi założeniami, zwracając uwagę na efektywność wdrożonych zabezpieczeń oraz wskazując obszary i kierunki potencjalnego doskonalenia SZBI. Każda stwierdzona podczas audytu niezgodność powinna zostać opisana w sposób jasny, jednoznaczny i zwięzły. Raport z niezgodności powinien zawierać w szczególności: opis sytuacji (faktu), dowody potwierdzające wystąpienie niezgodności, niespełnione wymagania, miejsce wystąpienia (komórka, dział) oraz stopień niezgodności (np. mała, średnia, duża).

Z perspektywy potencjalnych rezultatów, jakie dostarcza audyt systemu zarządzania wskazać można następujące jego funkcje [3, 9]:

- ***weryfikującą*** – dostarcza dowodów na to, czy utworzony i utrzymywany w organizacji system zarządzania jest zgodny z wymaganiami prawnymi, normatywnymi i innymi kryteriami wewnętrznymi;
- ***wartościującą*** – pozwala ocenić skuteczność systemu zarządzania, czyli stopień w jakim wpływa on na realizację celów przedsiębiorstwa;
- ***informacyjną*** – dostarcza kierownictwu, pracownikom oraz interesariuszom informacji odnośnie działania audytowanego systemu; wpływa także na proces decyzji na różnych szczeblach zarządzania;
- ***korygującą*** – w sytuacji stwierdzonych niezgodności umożliwia zaimplementowanie rozwiązań ukierunkowanych na wykrywanie i eliminowanie źródeł powstawania tych niezgodności;
- ***zapobiegawczą*** – podczas audytu zespół audytorski może zaobserwować potencjalne możliwości powstania niezgodności oraz wskazać propozycję działań profilaktycznych;
- ***instruktażową*** – w trakcie trwania audytu doświadczony audytor może podpowiedzieć audytowanemu pracownikowi właściwe sposoby postępowania, dobre praktyki itd.

- ***doskonalącą*** – audyt poprzez identyfikację luk i słabości występujących w systemie zarządzania pozwala także na wskazanie obszarów wymagających doskonalenia.

Należy jednak zaznaczyć, iż wyżej wymienione funkcje audytu możliwe są do osiągnięcia tylko i wyłącznie, gdy proces audytowy będzie realizowany zgodnie z określonymi standardami. Podstawowe zalecenia w zakresie przeprowadzania audytu systemu zarządzania zawarte zostały w normie ISO 19001:2012. Należą do nich następujące zasady [5, 7]:

- ***postępowanie etyczne*** – zaufanie, uczciwość, rzetelność, rozwaga, postawa profesjonalizmu;
- ***rzetelna prezentacja*** – jasne, transparentne, dokładne, zgodna z prawdą przedstawienie spraw;
- ***poufność*** – zachowanie poufności;
- ***niezależność*** – zasada bezstronności audytu oraz obiektywnych wniosków z audytu;
- ***podejście oparte na dowodach*** – zastosowanie racjonalnych metod badawczych, pozwalających na uzyskanie rzetelnych i powtarzalnych wniosków z audytu.

## 4. Etapy działań audytowych SZBI

Do podstawowych etapów działań audytowych SZBI zalicza się [2, 4, 6]:

- inicjowanie audytu;
- przegląd dokumentacji;
- przygotowanie działań audytowych;
- przeprowadzenie działań audytowych;
- przygotowanie i rozpowszechnienie raportu;
- przeprowadzenie działań poaudytowych (nie stanowią one części audytu, ale są niezmiernie ważne z uwagi na cel całego procesu audytowego).

### 4.1. Inicjowanie audytu

Pierwszym etapem badań w procesie audytowania SZBI jest *inicjowanie audytu*, na które składa się: wyznaczenie audytora wiodącego, określenie celów, zakresu i kryteriów audytu, określenie wykonalności audytu, wyznaczenie zespołu audytującego oraz wstępny kontakt z audytowanym.

*Audytorem wiodącym* zostaje wyznaczona osoba, która posiada odpowiednie kwalifikacje zawodowe (potwierdzone certyfikatem) oraz uprawnienia audytora wewnętrznego lub zewnętrznego. Audytor wiodący odpowiedzialny jest za przeprowadzanie audytu oraz przygotowanie raportu. Wyznacza go zarządzający programem audytów, z kolei audytor wiodący w konsultacji z zarządem audytowanego przedsiębiorstwa wybiera pozostałych członków zespołu audytującego oraz ewentualnych ekspertów technicznych w danej dziedzinie. Do odpowiedzialności i zadań audytora wiodącego należy w szczególności [5, 6]:

- opracowanie planu i zakresu audytu SZBI;
- przygotowanie dokumentacji roboczej (np. listy pytań kontrolnych) oraz instruktażu dla pozostałych audytorów;
- przegląd dokumentacji SZBI;
- reprezentowanie zespołu audytowego w rozmowach z audytowaną organizacją;
- kierowanie członkami zespołu audytowego;

- wspieranie audytorów – praktykantów;
- kierowanie zespołem w celu zrealizowania audytu;
- zapobieganie i usuwanie konfliktów;
- przygotowanie raportu z audytu.

W ramach ustalenia ogólnego programu audytów uwzględnić należy przede wszystkim: *cel, zakres i kryteria audytu*, które powinny zostać jasno wyrażone i udokumentowane. *Cel*, określa co ma być rezultatem przeprowadzonego audytu SZBI i może dotyczyć oceny zgodności SZBI z wymaganiami prawnymi i normatywnymi, oceny skuteczności oraz zdolności systemu, a także służyć może do identyfikacji obszarów wymagających doskonalenia. W przypadku ubiegania się o certyfikat zgodności z normą ISO/IEC 27001:2013 celem audytu będzie potwierdzenie tej zgodności. *Zakres audytu* opisuje obszar i granice audytu, takie jak: fizyczne lokalizacje, jednostki organizacyjne i procesy, które mają zostać poddane audytowi oraz ramy czasowe audytu. Z kolei *kryteria audytu* obejmują politykę, procedury, normy, przepisy prawne, wymagania systemu zarządzania, wymagania kontraktowe lub kodeksy postępowania branżowego lub biznesowego.

W fazie inicjacji audytu niezbędne jest także *określenie wykonalności audytu*, biorąc pod uwagę następujące czynniki [2, 4]:

- dostępność wystarczającej i odpowiedniej informacji do planowania audytu;
- możliwość współpracy z audytowanym;
- niezbędny czas i zasoby.

Oprócz tego, konieczne jest także *ustalenie wstępnych parametrów audytu*, do których zalicza się [5]:

- cele, zakres, kryteria i szacowany czas trwania audytu;
- kompetencje zespołu audytorskiego potrzebne do osiągnięcia celów audytu;
- wymagania wynikające z ustaw, zarządzeń, umów i akredytacji/certyfikacji;
- potrzebę zapewniania niezależności zespołu audytorskiego w celu uniknięcia konfliktu interesu;
- zdolność członków zespołu audytorskiego do efektywnego kontaktu i współpracy z audytowanym;
- język audytu;
- zrozumienie indywidualnych, społecznych i kulturowych cech audytowanego.

Przy *wyborze poszczególnych osób do zespoły audytorskiego* kluczowym jest zwrócenie uwagi na ich odpowiednie kwalifikacje zawodowe oraz kompetencje społeczne. Audytor powinien posiadać cechy osobowe pozwalające działać zgodnie z zasadami audytowania oraz wykazywać się zdolnością do stosowania wiedzy i umiejętności, niezbędnych do prowadzenia audytu. Zaleca się, aby osobę audytora charakteryzowały następujące cechy osobowościowe [5, 6]:

- ***etyczny*** – uczciwy, prawdomówny;
- ***otwarty*** – otwarty na poglądy innych;
- ***dyplomatyczny*** – taktowny w postępowaniu z innymi ludźmi;
- ***spostrzegawczy*** – świadomy otaczających go rzeczy;
- ***percepcyjny*** – świadomy sytuacji i zdolny do jej zrozumienia;
- ***elastyczny*** – przystosowujący się do różnych sytuacji;
- ***wytrwały*** – skupiony na osiągnięciu celów;
- ***zdecydowany*** – wyciągający w porę logiczne wnioski;
- ***niezależny*** – działający niezależnie, jednocześnie efektywnie współpracując z innymi;

- ***nieugięty***, odporny na presję – działający odpowiedzialnie i etycznie, nawet jeżeli te działania nie zawsze są popularne i mogą prowadzić do sporów;
- ***otwarty na doskonalenie***;
- ***wrażliwy na czynniki kulturowe***;
- ***chętny do współpracy***.

Ostatni krok w działaniu inicjującym audyt stanowi *nawiązanie kontaktu z audytowaną organizacją*. Jego celami są [2, 4, 6]:

- ustalenie sposobów komunikacji z przedstawicielem audytowanego;
- potwierdzenie upoważnienia do przeprowadzenia audytu;
- dostarczenie informacji w kwestii proponowanych terminów i składu zespołu audytorskiego;
- wnioskowanie o dostęp do odpowiednich dokumentów, w tym także zapisów;
- określenie wymagań i warunków bezpieczeństwa dla danego miejsca;
- dokonanie innych, istotnych z punktu przeprowadzania audytu ustaleń;
- uzgodnienie obecności obserwatorów oraz potrzeby przewodników dla członków zespołu audytorskiego.

Audyt swoim zakresem powinien obejmować wszystkie komórki organizacyjne odpowiedzialne za realizację podstawowych procesów biznesowych w przedsiębiorstwie oraz działy wspomagające, jak np. informatykę, kadry, finanse, księgowość itd. Oprócz tego proces audytu powinien być ukierunkowany na identyfikację przyczyn powstawania zagrożeń związanych z utratą poufności, integralności i dostępności informacji oraz uwzględniać wszystkie aktywa badanej jednostki, ze szczególnym uwzględnieniem informacji i ich nośników [6].

### 4.2. Przegląd dokumentacji

Przegląd dokumentacji dokonywany jest zazwyczaj u audytowanego i ma na celu weryfikację zgodności dokumentów SZBI z kryteriami audytu. Badaniu podlegają normatywne dokumenty SZBI, a także zapisy oraz raporty z poprzednich audytów. W szczególności przegląd dokumentacji SZBI powinien uwzględniać [6]:

- regulamin organizacji;
- schemat organizacyjny;
- misję oraz cele biznesowe przedsiębiorstwa;
- dokumenty regulujące zasady postępowania z informacjami (instrukcje, procedury, itd.);
- dokumenty dotyczące IT;
- plany postępowania w sytuacjach awaryjnych.

W przypadku, gdy przeprowadzony przegląd dokumentacji wykaże istotne braki i uchybienia organizacji w dokumentach, niezbędne jest dokonanie stosowanych korekt oraz uzupełnień. Oprócz tego, należy także rozważyć, czy audyt powinien być kontynuowany czy zostać zawieszony do czasu uporządkowania dokumentacji.

Analiza dokumentacji stanowi podstawę do oceny, w jaki sposób funkcjonuje SZBI, czy spełnia on określone wymagania normatywne i prawne oraz pozwala zespołowi audytorskiemu zapoznać się z podstawowymi procedurami postępowania i instrukcjami. Oprócz tego badanie stanu dokumentów pozwala stwierdzić ich zgodność z wymaganiami SZBI, w tym także może stanowić pierwsze, obiektywne dowody zgodności systemu z normą ISO/IEC 27001:2013 [6].

### 4.3. Przygotowanie działań audytowych

Na etap przygotowania działań audytowych składają się takie czynności jak: przygotowanie planu audytu przez audytora wiodącego, przydzielenie zadań poszczególnym członkom zespołu audytowego oraz opracowanie dokumentów roboczych.

*Opracowanie planu audytu* należy do podstawowych obowiązków audytora wiodącego. Plan ten ma za zadanie ustalenie terminów oraz koordynację działań audytora. Ilość szczegółów w nim zawartych w dużej mierze zależy od rodzaju i zakresu audytu (w zależności od tego czy jest to audyt certyfikujący czy kolejny audyt, zewnętrzny czy wewnętrzny).

Jednakże bez względu na rodzaj audytu – plan audytu powinien zawierać następujące informacje [5]:

- cele i kryteria audytu;
- informacje o kliencie;
- zakres audytu;
- daty i lokalizacje prowadzenia audytu;
- przewidywany czas trwania audytu;
- role oraz zakres odpowiedzialności poszczególnych członków zespołu audytorskiego;
- przydzielenie odpowiednich zasobów do krytycznych obszarów audytu.

Audytor wiodący ma także za zadanie *dokonać podziału zadań i odpowiedzialności* w zakresie audytowania określonych procesów SZBI, funkcji, miejsc, obszarów lub działań. Dokonując tego podziału audytor wiodący jest zobowiązany do zachowania niezależności, kwalifikacji i kompetencji audytorów oraz efektywnego wykorzystania zasobów.

Ponadto, w ramach realizacji etapu przygotowania audytu należy *opracować odpowiednią dokumentację roboczą*, którą obejmują m.in. listy kontrolne, plany próbkowania oraz formularze do zapisywania takich informacji jak: dowody pomocnicze, ustalenia z audytu, notatki ze spotkań. Przykładową listę kontrolną przedstawiono w tabeli 1.

Tab. 1. Przykładowa lista pytań audytowych

| **Lista pytań audytowych** | | | |
|---|---|---|---|
| **Cel audytu:** *znaleźć obiektywne dowody – A.9.2 Zarządzanie dostępem użytkowników* | | | |
| **Cel stosowania**: *zapewnienie autoryzowanego dostępu użytkownikom i przeciwdziałanie próbom nieautoryzowanego dostępu do systemu i usług* | | | |
| **Wymagania (pkt. normy)** | **Pytania** | Odpowiedzi | |
| | | Tak | Nie |
| A.9.2.1 | Czy ustanowiono formalny proces rejestracji i wyrejestrowania użytkowników, aby umożliwić przyporządkowanie praw dostępu? | | |
| A.9.2.2 | Czy wdrożono formalne zasady przyznawania dostępu użytkownikom poprzez nadanie i odbieranie praw dostępu dla wszystkich użytkowników do wszystkich systemów i usług? | | |
| A.9.2.3 | Czy przydzielanie i wykorzystywanie praw dostępu jest ograniczone i kontrolowane? | | |
| A.9.2.4. | Czy przydzielanie poufnych informacji uwierzytelniających jest kontrolowane przez formalny proces zarządzania? | | |

Źródło:[5]

### 4.4. Przeprowadzenie działań audytowych

Przeprowadzenie działań audytowych składa się z: przeprowadzenia spotkania otwierającego, ustalenia zasad komunikowania się podczas audytu (zarówno członków zespołu między sobą oraz autytorów z audytowanymi osobami), gromadzenia dowód audytowych, opracowania ustaleń audytu i przygotowania wniosków oraz przeprowadzenia spotkania zamykającego.

Pierwszym etapem prac związanych z przeprowadzaniem audytu jest *spotkanie otwierające*. Głównym jego celem jest zaprezentowanie audytowanym składu zespołu audytowego, omówienie metodyki przeprowadzania audytu oraz innych istotnych kwestii technicznych i organizacyjnych związanych z przebiegiem audytu. W szczególności spotkanie otwierające ma za zadanie [2, 4, 6]:

- potwierdzić plan audytu i jego zakres;
- dostarczyć krótkiego opisu sposobu przeprowadzania czynności związanych z audytem;
- potwierdzić kanały komunikacji;
- wyjaśnić zasady poufności i bezpieczeństwa informacji;
- umożliwić zadawanie pytań przez audytowanych;
- ustalić termin spotkania zamykającego.

Zasadniczym elementem działań audytowych jest *zbieranie oraz weryfikacja informacji* w celu poszukiwania dowodów z audytu. Oparte są one na odpowednim próbkowaniu. Właściwy dobór próbki dotyczy [5]:

- wyboru reprezentatywnych zabezpieczeń opisanych w normie ISO/IEC 27001:2013;
- wyboru reprezentatywnych próbek ze wszystkich głównych działań organizacji i systemu;
- zapewnienia prioritetowego traktowania szczególnie chronionych obszarów w organizaji (systemie);
- odpowiedniego dobrania ważnych wskaźników oceny;
- wybóru przez audytora tego, co będzie stanowiło „próbkę” oraz jej rozmiaru (rozmiar próbki musi dostarczać pewności, co do rzetelności audytu).

*Poszukiwanie dowodów z audytu* opiera się na następujacych źródłach informacji [5]:

- wywiady (spotkania ogólne, kluczowe osoby w organizacji);
- analiza dokumentacji (procedury, instrukcje);
- zapisy (monitoring, zapisy);
- obserwacje (rekonesans na miejscu).

*Uzyskane dowody z audytu poddaje się ocenie*, ukazując zgodność bądź niezgodność z kryteriami audytu oraz wskazując kierunki do doskonalenia. Po przeprowadzaniu badań audytowych zespół audytorski zbiera się w celu dokonania *przeglądu opracowanych ustaleń*. Następnie zespół audytorski przygotowuje *wnioski z audytu* w zakresie zgodności SZBI z kryteriami audytu, skuteczności wdrożenia, utrzymania i doskonalenia systemu. Wnioski z audytu powinny być jasne i zrozumiałe, a strona audytowana potwierdzić, że je otrzymała.

Ostatnim etapem przeprowadzania audytu jest *spotkanie zamykające*. Ma ono na celu przede wszystkim zaprezentowanie ustaleń z audytu oraz potwierdzenie przez audytowanych odnotowanych niezgodności. W trakcie spotkania zamykającego ustalane są także działania poaudytowe. Spotkanie zamykające ma przede wszystkim służyć [5]:

- omówieniu przebiegu audytu;

- zaprezentowaniu wniosków z audytu (wyników audytu);
- przedstawieniu ustaleń z audytu (niezgodności, spostrzeżeń, zaleceń);
- ustaleniu terminu przedstawienia planu działań poaudytowych.

W przedsiębiorstwach małych spotkanie zamykające może polegać jedynie na przedstawieniu ustaleń oraz wniosków z audytu.

### 4.5. Przygotowanie i rozpowszechnienie raportu

Raport z audytu powinien być kompleksowym, przejrzystym, odpowiednim zapisem ustaleń z audytu. Raport z audytu powinien zawierać [5]:

- cele audytu;
- zakres, przede wszystkim opis struktur w organizacji, których funkcjonowanie było przedmiotem audytu;
- identyfikację audytora (lub zespołu audytującego);
- terminy i miejsca prowadzenia audytu;
- kryteria audytu;
- wnioski z audytu (niezgodności, potencjały, uwagi);
- plan audytu;
- imienną listę uczestników.

Oprócz tego, raport z audytu może również zawierać takie informacje jak [5]:

- uwagi odnośnie przebiegu audytu (w szczególności powstałe bariery zakłócające przebieg audytu);
- obszary wyłączone z audytu;
- stopień realizacji audytu;
- rozbieżności w ocenie między zespołem audytowym, a stroną audytowaną;
- wskazówki do dalszych ulepszeń (potencjał poprawy);
- uzgodnione działania poaudytowe (follow-ups);
- zasady dystrybucji raportu.

Obowiązkiem audytora wiodącego jest dopilnowanie, aby strona audytowana otrzymała raport w wyznaczonym terminie. Należy podkreślić, iż dokument ten jest własnością audytowanej organizacji i należy zadbać o jego poufność oraz właściwe zabezpieczenie zarówno przez zespół audytowy, jaki i poszczególnych jego adresatów.

### 4.6. Przeprowadzenie działań poaudytowych

Jednostka audytowana, po otrzymaniu raportu z audytu zobligowana jest do zbadania przyczyn odnotowanych niezgodności i podjęcia określonych działań poaudytowych (korygujących, zapobiegawczych, doskonalących) w celu ograniczenia ponownego ich powstania w SZBI. Przedsięwzięcia te powinny zostać dokładnie zaplanowane oraz wdrożone w ustalonym czasie. Jeżeli jest to konieczne, działania poudytowe mogą wiązać się także z przeprowadzeniem audytu sprawdzającego [2, 4].

## 5. Przykłady niezgodności w systemie zarządzania bezpieczeństwem informacji z normą ISO 27001 – studium przypadku

*Niezgodność* oznacza niespełnione wymagania w stosunku do [5]:

- normy ISO/IEC 27001:2013;

- polityki SZBI;
- procedur i instrukcji SZBI;
- umów i przepisów;
- innych przyjętych ustaleń.

Norma ISO 19011:2012 wskazuje, że odnotowywane niezgodności mogą być stopniowane. Najczęściej wyróżnia się dwie rangi niezgodności:

- niezgodność dużą (krytyczną) – niezgodność, która powoduje brak skuteczności SZBI (systematyczne, celowe niespełnianie wymagań normy);
- niezgodność małą – niezgodność, która nie wpływa na skuteczność SZBI, (jednostkowy przypadek).

Ponadto, zidentyfikowane w SZBI słabości lub potencjalne słabości nie poparte obiektywnymi dowodami mogą zostać zapisane jako:

- potencjał doskonalenia – potencjalna możliwość doskonalenia badanego obszaru; aspekty pozwalające zoptymalizować SZBI w powiązaniu z wymaganiami normy ISO 27001:2013;
- obserwacja – zdarzenia, które zaniepokoiły w ocenie audytora SZBI, a audytor nie dostrzega możliwości doskonalenia; zapisuje on stan faktyczny na dzień przeprowadzania audytu w celu odnotowania sytuacji oraz jej obserwacji w przyszłości.

Poniżej przedstawiono przykłady niezgodności wraz z propozycją działań korygujących. Wdrożenie ich w przedsiębiorstwie pozwoli na uniknięcie powtarzania się tych niezgodności w przyszłości oraz uczyni system zarządzania bezpieczeństwem informacji odporniejszy na różnego rodzaju zagrożenia.

Tab. 2. Przykłady niezgodności z normą ISO/IEC 27001:2013.

a)

| Jednostka audytowana: *Dział Marketingu* | | |
|---|---|---|
| Klasyfikacja | Opis | Wymagania |
| *NZ duża* | *W trakcie audytu zaobserwowano, że dwa dokumenty: Umowa 220/2016 oraz Raport miesięczny X/2015 z oznaczeniem „Tajemnica Przedsiębiorstwa", pozostawione są na biurku bez nadzoru.* | *A.8.2.3 Postępowania z aktywami A. 11.2.9 Polityka czystego biurka i ekranu* |
| Działania korygujące/doskonalące:<br>*Przeprowadzono szkolenie pracowników ze szczególnym uwzględnieniem zasad czystego biurka i ekranu.* | | |

b)

| Jednostka audytowana: *Dział Księgowości* | | |
|---|---|---|
| Klasyfikacja | Opis | Wymagania |
| *NZ duża* | *Zatrudniony od 2 dni nowy pracownik oświadczył, że nie odbył szkolenia z zakresu SZBI, z kolei miał szkolenie z BHP oraz danych osobowych.* | *A.7.2.2 Uświadamianie, kształcenie, szkolenie z zakresu bezpieczeństwa informacji* |
| Działania korygujące/doskonalące:<br>*Pracownik został przeszkolony.*<br>*Po przeanalizowaniu sytuacji okazało się, że osoba odpowiedzialna w firmie za przeprowadzanie szkoleń z zakresu SZBI przebywała na zwolnieniu lekarskim. Wyznaczony został zastępca.* | | |

c)

| Jednostka audytowana: *Dział Handlowy* | | |
|---|---|---|
| Klasyfikacja | Opis | Wymagania |
| *NZ mała* | *W trakcie audytu stwierdzono obecność gościa, który nie posiadał wymaganego identyfikatora.* | *A.11.1.5 Praca w obszarach bezpiecznych* |
| Działania korygujące/doskonalące: *Identyfikatora nie wydano z powodu nieostrożności pracownika recepcji. Pouczono pracownika o jego obowiązku wydawania identyfikatorów oraz pilnowania ich zwrotu.* | | |

d)

| Jednostka audytowana: *Dział IT* | | |
|---|---|---|
| Klasyfikacja | Opis | Wymagania |
| *NZ mała* | *Firma rozpoczęła wdrażanie nowego systemu poczty elektronicznej Lotus Notes. Wcześniej korzystała z oprogramowania Exchange. Przed projektem nie opracowano wytycznych w zakresie bezpieczeństwa informacji. Wytyczne ten powstały po zakończeniu projektu. Wykonawca dostarczył raport.* | *A.14.2.7 Prace rozwojowe zlecane podmiotom zewnętrznym A.6.1.5. Bezpieczeństwo informacji w zarządzaniu projektami* |
| Działania korygujące/doskonalące: *W przyszłości zaleca się staranne i systematyczne nadzorowanie oraz monitorowanie przez firmę prac i zadań powierzanych podmiotom zewnętrznym.* | | |

e)

| Jednostka audytowana: *Dział Marketingu* | | |
|---|---|---|
| Klasyfikacja | Opis | Wymagania |
| *PD* | *Na komputerze stwierdzono nieaktualne oprogramowanie antywirusowe. Po wymuszeniu aktualizacji ręcznie poprzez użytkownika, program zainstalował aktualne poprawki i bazę subskrypcji antywirusowej. Użytkownik oświadczył, że w ciągu ostatnich 2 miesięcy nie było żadnych alertów z informacją o wykrytym zagrożeniu.* | *A.12.2.1 Zabezpieczenie przed szkodliwym oprogramowaniem* |
| Działania korygujące/doskonalące: *Dokonano przeglądu oprogramowania antywirusowego na wszystkich stacjach roboczych wraz z funkcją automatycznej aktualizacji oraz zalecono pracownikom zadbanie o regularną aktualizację oprogramowania oraz systemu operacyjnego komputera.* | | |

f)

| Jednostka audytowana: *Dział Serwisu* | | |
|---|---|---|
| Klasyfikacja | Opis | Wymagania |
| *PD* | *Brygady remontowe zabierają ze sobą dużą ilość dokumentacji papierowej, Istnieje możliwość zaistnienia incydentu bezpieczeństwa informacji (np. zgubienie bądź zniszczenie dokumentów). Do tej pory nie odnotowano żadnego incydentu.* | *6.1.3 Postępowanie z ryzykiem BI A.8.2.3 Eksploatacja zasobów* |
| Działania korygujące/doskonalące: *Opracowano i wdrożono zasady bezpiecznego wynoszenia mienia poza organizację, w tym zasady postępowania z dokumentami przetwarzanymi poza terenem organizacji.* | | |

g)

| Jednostka audytowana: *Sekretariat* | | |
|---|---|---|
| Klasyfikacja | Opis | Wymagania |
| *OB* | *Podczas rozmowy z praktykantem okazało się, że* | *A. 8.1.3* |

| | | |
|---|---|---|
| | *przygotowuje on nową dokumentację techniczną celem przedłożenia oferty dla klienta.* | *Akceptowalne użycie informacji* |
| Działania korygujące/doskonalące:<br>*Uszczegółowiono zasady korzystania z aktywów przez praktykantów i stażystów zatrudnionych w organizacji wraz z ustanowieniem osób odpowiedzialnych za te zasoby.*<br>*Obserwacja odnotowana w raporcie. Do sprawdzenia podczas następnego audytu.* | | |

h)

| Jednostka audytowana: *Dział Strategii i Planowania* | | |
|---|---|---|
| Klasyfikacja | Opis | Wymagania |
| *OB* | *W trakcie rozmowy z administratorami systemu PLAN okazało się, że mają oni zbyt dużo zadań do realizacji i nie mają czasu na opracowanie własnych usprawnień w systemie PLAN, w tym także dotyczących BI.* | *7.1. Zasoby* |
| Działania korygujące:<br>*Kierownik grupy administratorów dokonał przeglądu obowiązków i zadań administratorów.*<br>*Administratorzy rozpoczęli pracę nad wprowadzaniem usprawnień do systemu PLAN.*<br>*Obserwacja odnotowana w raporcie. Do sprawdzenia podczas następnego audytu.* | | |

Źródło: opracowanie własne na podstawie [5]

Z przytoczonych niezgodności wynika, iż źródłem ich powstawania może być m.in. niedostateczne zaangażowanie kierownictwa, niewłaściwe zarządzanie zasobami potrzebnymi dla SZBI (w tym czasem), zaniedbania pracowników czy luki i niedociągnięcia w procedurach i instrukcjach postępowania.

## 6. Podsumowanie

Współczesne organizacje silnie uzależnione są informacji. Stanowią one ważne aktywa biznesowe, niezbędne do zachowania konkurencyjnej pozycji na rynku, płynności finansowej, zyskowności, a także dobrej renomy organizacji. Stąd też identyfikacja potrzeb, osiągnięcie odpowiedniego poziomu oraz utrzymanie i doskonalenie bezpieczeństwa informacji jest niezmiernie ważnym zadaniem.

Fundamentem każdego systemu bezpieczeństwa informacji powinna być wiedza praktyczna pochodząca z wielu źródeł, w tym od instytucji badawczych oraz producentów systemów zabezpieczeń. Standardem opartym o dobre praktyki jest norma ISO/IEC 27001:2013, która wskazuje, w jaki sposób zbudować system bezpieczeństwa informacji w organizacji oraz jak go należy utrzymywać, adaptować do zmienianego się otoczenia i doskonalić. Przytoczona norma zawiera propozycję różnego rodzaju zabezpieczeń technicznych i rozwiązań organizacyjnych niezbędnych do stworzenia systemu ochrony zasobów przed szeroką gamą zagrożeń.

Podstawą skuteczności funkcjonowania takiego systemu są audyty wewnętrzne, które pozwalają wykryć potencjalne niezgodności i zagrożeń oraz podjąć działania profilaktyczne i usprawniające. Stąd też można wnioskować, iż audyt jest z jednej strony instrumentem diagnostycznym, z drugiej zaś strony doskonalącym.

Należy jednak podkreślić, iż osiągnięcie wymiernych korzyści z audytu wymaga, aby proces ten przeprowadzonych był zgodnie z określonymi standardami. Podstawowe wymagania w zakresie przeprowadzania audytu definiuje norma ISO 19011:2012. Zawiera ona wytyczne odnoszące się do zarządzania programami audytów, sposobu realizacji działań audytowych oraz kompetencji audytorów.

**Literatura**


1. Hebelman J., Audyt zintegrowanego systemu zarządzania w świetle wymagań ISO w przedsiębiorstwie X [w:] Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse, Rynki Finansowe, Ubezpieczenia Nr 76, t. 2/2015.
2. Janczak J., Nowak A., Bezpieczeństwo informacyjne. Wybrane problemy, Wyd. AON, Warszawa 2013.
3. Jedynak P. (red.), Audyt w zarządzaniu przedsiębiorstwem, Wyd. Księgarnia Akademicka, Kraków 2004.
4. Łuczak J., Tyburski M., Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001, Wyd. Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2010.
5. Materiały szkoleniowe Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001:2013, Wyd. TÜV NORD, Katowice 2015.
6. Nowak A., Scheffes W., Zarządzanie bezpieczeństwem informacyjnym, Wyd. AON, Warszawa 2010.
7. PN-ISO 19011:2012 Wytyczne dotyczące audytowania systemów zarządzania, Wyd. PKN, Warszawa 2012.
8. PN-ISO/IEC 27001:2013 Technika informatyczna. Techniki bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji. Wymagania, Wyd. PKN, Warszawa 2014.
9. Toruński J., Znaczenie audytu w procesie zarządzania jakością w przedsiębiorstwie, [w] Zeszyty Naukowe Uniwersytetu Przyrodniczo – Humanistycznego w Siedlcach. Seria Administracja i Zarządzanie Nr 98/2013.
10. Urbaniak M., Zarządzanie jakością – teoria i praktyka, Warszawa 2004.
11. Wolska E., Audyt zgodności z normą ISO/IEC 27001:2005 [w] Zeszyty Naukowe Warszawska Wyższa Szkoła Informatyki Nr 7/15.
12. Wołowski F., Zawiła – Niedźwiecki J., Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, Wyd. edu-Libri, Kraków-Warszawa 2012.



Dr inż. Michał PAŁĘGA
Dr hab. inż. Marcin KNAPIŃSKI, prof. PCz.
Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa
Wydział Inżynierii Produkcji i Technologii Materiałów
Politechnika Częstochowska
42 – 201 Częstochowa, Dąbrowskiego 69
tel./fax: (034) 325 07 82
e-mail: mpalega@wip.pcz.pl
knap@wip.pcz.pl