

Małgorzata Wilczyńska¹

Państwowa Akademia Nauk Stosowanych im. ks. Bronisława Markiewicza
w Jarosławiu

Justyna Wilczyńska-Baraniak²

https://doi.org/10.29316/9788368103359_5

AUDYT BEZPIECZEŃSTWA INFORMACJI

INFORMATION SECURITY AUDIT

Streszczenie

W dobie cyfrowej transformacji i rosnących zagrożeń w cyberprzestrzeni, bezpieczeństwo informacji stało się kluczowym aspektem funkcjonowania każdej organizacji. Bezpieczeństwo informacji jest kluczowym elementem strategii organizacji, wymagającym ciągłej uwagi, inwestycji i doskonalenia w obliczu zmieniającego się krajobrazu zagrożeń cybernetycznych. Skuteczne zarządzanie bezpieczeństwem informacji wymaga kompleksowego podejścia, łączącego technologię, procesy i ludzi. Bezpieczeństwo informacji jest kwestią niezwykle ważną w kontekście każdego działania, dlatego organizacje powinny zadbać nie tylko o procedury i polityki bezpieczeństwa, ale też o systematyczne audyty. Audyt to systematyczny, niezależny

¹ <https://orcid.org/0000-0002-1969-3498>, e-mail: malgorzata.wilczynska@pansjar.edu.pl

² <https://orcid.org/0009-0005-3148-8197>, e-mail: justaw@o2.pl

i udokumentowany proces uzyskiwania dowodów z audytu oraz ich obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu. Audyt bezpieczeństwa informacji, to kompleksowa analiza systemów IT, procedur, polityk oraz zabezpieczeń w organizacji, mająca na celu ocenę poziomu ochrony danych i zgodności z obowiązującymi standardami. Nie jest to wyłącznie techniczne badanie infrastruktury – dobry audyt uwzględnia także czynnik ludzki, dokumentację i kulturę organizacyjną w zakresie bezpieczeństwa. Z jednej strony audyt bezpieczeństwa informacji daje odpowiedź na pytanie, czy organizacja spełnia obowiązki formalne, a z drugiej analizuje wymagania techniczne dotyczące systemów informatycznych, przy pomocy których informacje są przetwarzane. Regularne przeprowadzanie audytów bezpieczeństwa jest kluczowe dla utrzymania wysokiego poziomu ochrony danych i systemów informatycznych, co pomaga organizacjom przeciwdziałać potencjalnym zagrożeniom oraz reagować na incydenty bezpieczeństwa w odpowiedni sposób. Ze względu na ciągle zmieniające się przepisy i coraz większe oczekiwania związane z bezpieczeństwem, a także pojawiające się zagrożenia, jest wskazane, aby cyklicznie przeprowadzać audyt i na bieżąco weryfikować stosowane zabezpieczenia. Regularne audyty pozwalają zidentyfikować ryzyka związane z utratą lub ujawnieniem danych oraz wdrożyć odpowiednie środki zapobiegawcze. Celem rozdziału jest przedstawienie roli audytu bezpieczeństwa informacji, procesu audytowania oraz wskazanie podstawowych zasad audytowania. Treści prezentowane w rozdziale opracowano z wykorzystaniem teoretycznych metod badawczych, wiodącą z nich była analiza krytyczna literatury przedmiotu, analiza kwerendy źródeł internetowych, jak również metoda analizy, syntezy, uogólnienia oraz wnioskowania.

Słowa kluczowe: bezpieczeństwo informacji, audyt, jakość audytu, proces audytowania

Abstract

In the era of digital transformation and growing threats in cyberspace, information security has become a key aspect of every organization's operations. Information security is a key element of an organization's strategy, requiring constant attention, investment, and improvement in the face of a changing cyber threat landscape. Effective information security management requires a comprehensive approach that combines technology, processes, and people. Information security is an extremely important issue in the context of any activity, which is why organizations should ensure not only security procedures and policies, but also systematic audits. An audit is a systematic, independent, and documented process of obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are met.

An information security audit is a comprehensive analysis of an organization's IT systems, procedures, policies, and security measures to assess the level of data protection and compliance with applicable standards. It is not just a technical examination of infrastructure – a good audit also takes into account the human factor, documentation, and organizational culture in terms of security. On the one hand, an information security audit answers the question of whether an organization meets its formal obligations, and on the other hand, it analyzes the technical requirements for the IT systems used to process information. Regular security audits are crucial for maintaining a high level of data and IT system protection, helping organizations counteract potential threats and respond to security incidents in an appropriate manner. Due to constantly changing regulations and increasing security expectations, as well as emerging threats, it is advisable to conduct regular audits and verify the security measures in place on an ongoing basis. Regular audits allow you to identify risks related to data loss or disclosure and implement appropriate preventive measures. The purpose of this chapter is to present the role of information security auditing, the auditing process, and to indicate the basic principles of auditing. The content presented in the chapter was developed using theoretical research methods, the leading one being a critical analysis of the literature on the subject, an analysis of online sources, as well as the methods of analysis, synthesis, generalization, and inference.

Keywords: information security, audit, audit quality, auditing process

Wstęp

W dobie cyfrowej transformacji i rosnących zagrożeń w cyberprzestrzeni, bezpieczeństwo informacji stało się kluczowym aspektem funkcjonowania każdej organizacji. Bezpieczeństwo informacji jest kwestią niezwykle ważną w kontekście każdego działania, dlatego organizacje powinny zadbać nie tylko o procedury i polityki bezpieczeństwa, ale też o systematyczne audyty. Audyt bezpieczeństwa informacji to systematyczny i kompleksowy przegląd procedur i polityki bezpieczeństwa. Taki audyt wiąże się z realną i wymierną oceną, czy organizacja stosuje skuteczne działania prewencyjne chroniące m.in. przed wyciekami danych i cyberatakami. Na koniec prac przygotowujemy jest raport, w którym wypisane są stwierdzone niezgodności, a także wskazówki, co zrobić, aby system bezpieczeństwa informacji był szczelny i odporny na zagrożenia (Klichowski, b.d.). Rolą

audytu jest weryfikacja poprawności stosowanych zabezpieczeń w odniesieniu do założonych wymagań. Sam audyt jest procesem, prowadzonym przez niezależną jednostkę, która gromadzi i ocenia materiały funkcjonujące w organizacji i bada je pod kątem zgodności z ustalonymi kryteriami np. przepisami prawa, normami czy politykami bezpieczeństwa (Borkowski, b.d.). Zapewnienie bezpieczeństwa informacji jest kwestią bardzo ważną nie tylko dla podmiotów publicznych, ale i mniejszych organizacji. Każda organizacja narażona jest na ataki z zewnątrz, które mogą narazić ją na utratę zaufania i ogromne straty finansowe. Dlatego też powinna mieć wprowadzone procedury i polityki bezpieczeństwa, które powinny być cyklicznie sprawdzane – tylko wtedy zyska pewność, że stosowane zabezpieczenia są poprawne i adekwatne do założonych wymagań. Jednym z najbardziej skutecznych narzędzi do takiej weryfikacji jest audyt bezpieczeństwa informacji. Skuteczne funkcjonowanie SZBI w organizacji wymaga prowadzenia audytów mających na celu weryfikację poprawności stosowanych zabezpieczeń w odniesieniu do założonych wymagań. Audyt bezpieczeństwa informacji sprawdza poziom bezpieczeństwa systemu zarządzania bezpieczeństwem informacji (SZBI). Warto wspomnieć, że międzynarodowym standardem systemu zarządzania bezpieczeństwem informacji jest ISO/IEC 27001. Norma ta nie tylko określa wymagania i zasady inicjowania, wdrażania, utrzymywania i poprawy zarządzania bezpieczeństwem informacji, ale też najlepsze praktyki odnoszące się do stosowania zabezpieczeń (Klichowski, b.d.). Audyt jest procesem, w którym niezależna jednostka gromadzi i ocenia dowody o różnicach między wartością wskaźników mierzalnych a ustalonymi kryteriami. Organizacja powinna przeprowadzać wewnętrzne audyty SZBI w zaplanowanych odstępach czasu, aby określić, czy cele stosowania zabezpieczeń, same zabezpieczenia, procesy i procedury są:

- zgodne z zaleceniami standardów i odpowiednimi ustawami i przepisami,
- zgodne z zidentyfikowanymi wymaganiami bezpieczeństwa informacji
- skutecznie wdrożone i utrzymywane,
- adekwatne do zidentyfikowanych zagrożeń i poziomów ryzyka (należy uwzględnić nowe zagrożenia i nowe rodzaje ryzyka),
- zgodne z oczekiwaniami.

Z jednej strony audyt bezpieczeństwa informacji daje odpowiedź na pytanie, czy organizacja spełnia obowiązki formalne, a z drugiej analizuje wymogi techniczne dotyczące systemów informatycznych, przy pomocy których informacje są przetwarzane. Program audytu należy zaplanować, biorąc pod uwagę status i ważność procesów oraz ulokowanie obszarów wskazanych do audytu, jak również wyniki poprzednich audytów. Kryteria audytu, zakres, częstotliwość i metody powinny być zdefiniowane. Każdy audyt musi mieć wyznaczony cel (czyli co należy osiągnąć w następstwie audytu), kryteria (przepisy prawne, zarządzenia, procedury SZBI), zakres (obejmuje jednostki organizacyjne, fizyczne lokalizacje, procesy, działania) oraz termin wykonania. Audyt bezpieczeństwa informacji to systematyczny i kompleksowy przegląd procedur i polityki bezpieczeństwa; wiąże się z realną i wymierną oceną, czy organizacja stosuje skuteczne działania prewencyjne chroniące m.in. przed wyciekiem danych i cyberatakami. Działania audytorskie, a więc prowadzenie audytu bezpieczeństwa informacji, to systematyczny proces oceny i przeglądu procedur, polityk i systemów informatycznych organizacji w celu weryfikacji ich skuteczności i zgodności z normami i przepisami. Obejmuje on planowanie, zbieranie dowodów, analizę danych, a następnie przygotowanie raportu z rekomendacjami dotyczącymi poprawy poziomu bezpieczeństwa (raport, w którym wypisane są stwierdzone niezgodności, a także wskazówki, co zrobić, aby system bezpieczeństwa informacji był szczelny i odporny na zagrożenia). Przeprowadza się również spotkanie zamykające audytu, na którym przedstawiany jest raport wraz z rekomendacjami. Działania audytowe pomagają zidentyfikować luki w zabezpieczeniach, zapobiec cyberatakowi i ochronić dane przed utratą, zapewniając tym samym ciągłość działania i minimalizując ryzyko strat finansowych. Audyt definiuje się jako systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów i ich obiektywnej oceny w celu określenia stopnia spełnienia założonych kryteriów. Wybór audytorów i sposób przeprowadzenia audytu powinny zapewnić obiektywność i bezstronność procesu audytowego. Audyt powinna wykonać jednostka zewnętrzna, aby zyskać gwarancję rzetelnej, bezstronnej i miarodajnej oceny. Audytorzy nie powinni audytować swojej własnej pracy. Audytor nie powinien także audytować obszaru, co do którego istnieje podejrzenie, że będzie miał trudności z zachowaniem obiektywizmu. Jest to ważne, bowiem celem audytora jest uzyskanie dowodów z audytu i wydanie obiektywnej oceny, która

pozwole określić stopień spełnienia kryteriów. Celem audytorów jest szukanie zgodności, a nie poszukiwanie potknięć audytowanego. Audytorzy nie mogą kierować się negatywnymi emocjami wobec audytowanego. Audytorzy muszą pamiętać, że audyt nie jest kontrolą. Nie mogą zapominać, że audyty wewnętrzne podejmowane są dobrowolnie przez organizację i ich celem jest doskonalenie systemu. Audyt bezpieczeństwa może być realizowany zarówno przez osoby zatrudnione w weryfikowanej organizacji jak i za pomocą zewnętrznych specjalistów. Cechą audytu zewnętrznego jest niezależność oceny. Wprawdzie taki audyt można wykonać własnymi siłami (przez pracowników), ale zdecydowanie lepiej jest powierzyć to zadanie niezależnej i bezstronnej jednostce. Po pierwsze, gwarantuje to obiektywność audytu. Po drugie, instytucja audytująca ma niezbędne narzędzia oraz wiedzę o obowiązujących normach. Z kolei audyt wewnętrzny gwarantuje dobrą znajomość specyfiki organizacji i pozwala dokładnie analizować wybrane zabezpieczenia, ponieważ może być realizowany częściej niż audyt zewnętrzny. Aby dobrze wykonać zadanie audytorzy powinni rozumieć obszar audytowany i działalność audytowanego. Regularne przeprowadzanie audytów bezpieczeństwa jest kluczowe dla utrzymania wysokiego poziomu ochrony danych i systemów informatycznych, co pomaga organizacjom przeciwdziałać potencjalnym zagrożeniom oraz reagować na incydenty bezpieczeństwa w odpowiedni sposób. Jest wiele miejsc, w których można wykonać audyt. Audyt to pojęcie spotykane względnie często, choć tak naprawdę nie ma jednoznacznej definicji. Dodatkowo często mylone jest z kontrolą lub błędnie nazywane „auditem”. Kluczową trudnością w dokładnym ujęciu terminu „audyt” jest mnogość jego definicji. Co się z tym wiąże, nieraz pojawiają się nieścisłości w zakresie różnych jego klasyfikacji czy etapów przeprowadzania. Audyt – jedno z kluczowych wymagań systemów zarządzania opartych o normy ISO, którego celem jest ocena systemu, procesu, dostawcy. Audyt – zgodnie z definicją tego terminu – powinien być niezależnym, systematycznym procesem, którego celem jest ocena stopnia spełnienia określonych wymagań. Jeśli chodzi o oficjalne definicje, jedna z nich została zawarta w normie PN-EN ISO 19011:2018, która opisuje audytowanie systemów zarządzania, zasady jego przeprowadzania i zarządzania tego typu programami. Zgodnie z nią audyt to: „systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu obiektywnego oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów

audytu”. Generalnie zatem uznaje się, że audyt to szczegółowe badanie (analiza działalności) wybranej jednostki, które wykonują odpowiednio do tego przygotowani audytorzy. Często jest to proces, który powtarza się regularnie i ma duże znaczenie dla kontrolowania sytuacji panującej w danej jednostce, jej postępowania względem zgodności z prawem, wskazywania jej mocnych oraz słabych stron czy tworzenia planów na przyszłość. Audyt wewnętrzny to niezależna, obiektywna ocena, która pomaga organizacji ocenić jej procesy, mechanizmy kontroli i systemy, aby zapewnić skuteczne zarządzanie wydajnością, ryzykiem i zgodnością z przepisami. Można go traktować jako sposób na utrzymanie wszystkiego pod kontrolą, aby organizacja realizowała swoje cele i unikała potencjalnych problemów operacyjnych (Highspring, 2025). Audyt ma być narzędziem wspomagającym a nie kontrolnym, przeszkadzającym i nic nie wnoszącym dla doskonalenia organizacji. Audyt polega na weryfikacji zgodności w oparciu o obiektywne dowody. Celem jest znalezienie dowodów zgodności a nie doszukiwania się niezgodności. Audyt nie ocenia ludzi, lecz funkcjonowanie systemu/procesu. Nie może się odbyć bez audytowanego (Akademia Jakości, b.d.). Audyt to systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów z audytu oraz ich obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu. Audyt jest sprawdzeniem, czy wszystkie procedury w organizacji i posiadane dokumenty są zgodne z obowiązującym prawem i przyjętymi standardami bezpieczeństwa systemów. Ta kontrola jest połączona z analizą zarówno miejsca, jak i całego funkcjonującego systemu w miejscu audytowanym. Kompleksowy audyt bezpieczeństwa będzie wskazywać mocne i słabe strony organizacji. Wskaże również niezgodności – jeżeli występują. Z działań audytowych powstaje raport, którego analiza, a także wdrożenie zaleceń i działań poaudytowych da realną poprawę poziomu bezpieczeństwa. Należy też dodać, że każdy audyt powinien mieć jasno określone ramy czasowe, a jego sposób przeprowadzenia opierać się o bardzo konkretne procedury. Audyty bezpieczeństwa przeprowadza się m.in. w oparciu o normę ISO/IEC 27001, Ustawę o Krajowym Systemie Cyberbezpieczeństwa oraz Krajowe Ramy Interoperacyjności (Jurkiewicz, 2023). Jednostki publiczne mają obowiązek m.in.:

- przeprowadzania okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji (tzw. audytu KRI). Audyt KRI to kompleksowy proces weryfikacji zgodności systemów teleinformatycznych

i procesów organizacyjnych z wymaganiami Krajowych Ram Interoperacyjności,

- zgłaszania incydentów naruszenia bezpieczeństwa informacji,
- zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.

Można wnioskować, iż celem audytu jest dokładna i niezależna ocena danej organizacji, projektu, systemu, procesu, usługi czy nawet konkretnego produktu oraz wyszukanie wszelkich związanych z tym problemów. Ma to przynieść wiarygodne informacje, które w efekcie mają za zadanie pomóc w zarządzaniu określonym obszarem. Audyt zwykle ma zatem także charakter doradczy, czego finalnym celem jest wsparcie zarządzania organizacją i doprowadzenie do poprawy oraz usprawnienia działalności określonego podmiotu. Celem audytu jest potwierdzenie prawidłowego działania systemów bezpieczeństwa funkcjonujących w organizacji. Wszelkie raporty powstałe podczas audytu są przekazywane do osób upoważnionych oraz do instytucji państwowych, jeśli tak wymaga prawo. Ze względu na ciągle zmieniające się przepisy i coraz większe oczekiwania związane z bezpieczeństwem, a także pojawiające się zagrożenia, zaleca się cyklicznie przeprowadzać audyt i na bieżąco weryfikować stosowane zabezpieczenia.

Bezpieczeństwo informacji w organizacji

W dzisiejszym cyfrowym świecie informacja stała się jednym z najcenniejszych zasobów każdej organizacji. Bezpieczeństwo informacji to kompleksowe podejście do ochrony danych, które wykracza daleko poza tradycyjne zabezpieczenia techniczne. Obejmuje ono całokształt działań organizacyjnych, prawnych i technicznych mających na celu zapewnienie ochrony informacji przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem. Bezpieczeństwo informacji jest kluczowym aspektem ochrony danych osobowych i organizacyjnych przed nieautoryzowanym dostępem, ujawnieniem i naruszeniem. W obliczu rosnącej cyberprzestępczości i stale pojawiających się nowych zagrożeń, zarządzanie bezpieczeństwem informacji w każdej organizacji jest kluczowym elementem strategicznym i jednocześnie może wydawać się trudne lub wręcz niemożliwe. Zapewnienie bezpieczeństwa informacji

jest jednym z najważniejszych obszarów działania wszystkich organizacji oraz oddziaływania społecznego w rozwiniętych cywilizacyjnie i technologicznie krajach. Wraz ze wzrostem zagrożenia cyberatakami i coraz większym wykorzystaniem technologii cyfrowych, niezbędne stało się wdrożenie solidnych środków bezpieczeństwa informacji. Bezpieczeństwo informacji obejmuje różne strategie i procesy mające na celu ograniczanie ryzyka i ochronę poufnych informacji. Praktyczną cechą informacji jest to, że raz ujawniona niemal zawsze nie może już zostać powtórnie objęta ochroną, czyli pole zapewnienia ciągłości działania niemal nie istnieje. Działania podejmowane na rzecz ochrony i zarządzania bezpieczeństwem informacji powinny być kluczowe dla każdej organizacji a ich dobór powinien być proporcjonalny do zmieniającego się środowiska funkcjonowania podmiotu. W dzisiejszym świecie, gdzie informacje są kluczowym zasobem, bezpieczeństwo informacji ma ogromne znaczenie dla funkcjonowania organizacji, ochrony prywatności danych oraz utrzymania stabilności systemów informatycznych. W odniesieniu do opinii ekspertów, bezpieczeństwo wyraża się we wszystkich obszarach działalności organizacji. Jego struktura jest w istocie równoważna ze strukturą funkcjonowania podmiotu, zaś bezpieczeństwo informacyjne jest umiejscawiane, obok bezpieczeństwa publicznego, ekonomicznego i militarnego w ramach szerszych pojęć bezpieczeństwa międzynarodowego i narodowego (Koziej, 2011, s. 256). Bezpieczeństwo informacji (infosec) definiowane jest jako „stan i proces, w ramach którego zapewnia się w całym cyklu życia informacji (powstanie, przekazanie, przetworzenie, kopiowanie, wykorzystywanie, przechowywanie, gromadzenie, niszczenie), osiąganie i utrzymywanie z uwzględnieniem obowiązujących standardów bezpieczeństwa na pożądanym przez dany podmiot poziomie, takich jej fundamentalnych właściwości jak: dostępność, użyteczność, integralność i poufność” (Fehler, 2016, s. 30). Bezpieczeństwo informacji to kompleksowe podejście do ochrony danych i systemów informatycznych przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem. Jest to kluczowy element zarządzania ryzykiem informacyjnym w organizacjach, mający na celu zapewnienie poufności, integralności i dostępności informacji. Bezpieczeństwo informacji obejmuje zestaw zasad, procedur, narzędzi i praktyk mających na celu ochronę informacji w całym cyklu ich życia. Dotyczy to zarówno danych przechowywanych w formie elektronicznej, jak i papierowej. Celem

jest zapewnienie, że informacje są chronione przed różnymi zagrożeniami, zarówno wewnętrznymi, jak i zewnętrznymi (Widomski, 2026). Bezpieczeństwo informacji można także zdefiniować jako systematyczne podejście do zarządzania kluczowymi informacjami organizacji w celu zagwarantowania racjonalnego poziomu ich bezpieczeństwa. Obejmuje ono ludzi, procesy oraz technologię - obecnie nie można bowiem ograniczać się do bezpieczeństwa danych gromadzonych i przetwarzanych w systemach informatycznych. Bezpieczeństwo informacji jest kluczowym elementem strategii organizacji, wymagającym ciągłej uwagi, inwestycji i doskonalenia w obliczu zmieniającego się krajobrazu zagrożeń cybernetycznych. Skuteczne zarządzanie bezpieczeństwem informacji wymaga kompleksowego podejścia, łączącego technologię, procesy i ludzi. Obecnie stanowi ono złożony ekosystem, w którym równie istotne są aspekty technologiczne, jak i czynnik ludzki. Bezpieczeństwo informacji to nie tylko zabezpieczenia techniczne, ale również:

- aspekty organizacyjne: obejmują one polityki bezpieczeństwa, procedury, szkolenia pracowników i zarządzanie ryzykiem,
- aspekty prawne: zgodność z przepisami dotyczącymi ochrony danych, np. w Europie (Rada Europejska Rada Unii Europejskiej, 2024) obejmuje przede wszystkim Ochronę Danych Osobowych, regulowaną przez przepisy takie jak RODO (Urząd Ochrony Danych Osobowych, UODO (2022), które przyznają osobom fizycznym większą kontrolę nad ich danymi, narzucając na organizacje obowiązek bezpiecznego, transparentnego i zgodnego z prawem ich przetwarzania.

Obejmuje ono całokształt działań organizacyjnych, prawnych i technicznych mających na celu zapewnienie ochrony informacji przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem. W praktyce oznacza to konieczność wdrożenia kompleksowych rozwiązań, które uwzględniają zarówno zabezpieczenia systemów informatycznych, jak i odpowiednie procedury organizacyjne oraz szkolenia pracowników.

W swojej istocie bezpieczeństwo informacji koncentruje się na zapewnieniu trzech kluczowych aspektów: poufności, integralności oraz dostępności informacji, które wspólnie tworzą tak zwaną triadę CIA (Confidentiality, Integrity, Availability). Jest to kluczowy element zarządzania ryzykiem

informacyjnym w organizacjach, mający na celu zapewnienie poufności, integralności i dostępności informacji. W praktyce bezpieczna informacja oznacza, że muszą być spełnione trzy zasadnicze atrybuty ochrony informacji (Syta, 2025, s. 41):

- poufność (ang. *Confidentiality*) – czyli zapewnienie, że informacje są dostępne tylko dla osób uprawnionych do ich dostępu. Systemy i użytkownicy muszą być weryfikowani, aby utrzymać poufność danych,
- integralność (ang. *Integrity*) – czyli zagwarantowanie dokładności i kompletności informacji, oraz metod ich przetwarzania; oznacza utrzymanie dokładności, spójności i nienaruszalności danych przez cały ich cykl życia. Informacje nie mogą być modyfikowane w sposób nieautoryzowany,
- dostępność (ang. *Availability*) – czyli zapewnienie upoważnionym użytkownikom dostępu do informacji i związanych z nimi zasobów, zgodnie z określonymi potrzebami. Gwarantuje, że upoważnieni użytkownicy mają dostęp do potrzebnych informacji i zasobów w odpowiednim czasie (Malon Group, b.d).

Trzy koncepcje tj. poufność, integralność i dostępność stanowią fundament silnej ochrony informacji, tworząc podstawę infrastruktury zabezpieczeń organizacji. Dodatkowo, często uwzględnia się również takie własności jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Dodatkowe własności bezpieczeństwa informacji:

- autentyczność: weryfikuje tożsamość użytkowników i systemów, potwierdzając, że są oni tym, za kogo się podają; oznacza, że informacja pochodzi ze wskazanego źródła,
- niezaprzeczalność (ang. *Non-repudiation*): pozwala na udowodnienie, że określone działania lub zdarzenia miały miejsce, a użytkownik nie może zaprzeczyć swojej aktywności,
- rozliczalność (ang. *Accountability*): oznacza możliwość przypisania działań konkretnym podmiotom (osobom lub systemom), co pozwala na śledzenie ich aktywności,
- niezawodność (ang. *Reliability*): zapewnia, że systemy i dane działają w przewidywalny sposób, bez nieoczekiwanych awarii czy zakłóceń.

„Kluczowe zasady bezpieczeństwa informacji opierają się na modelu warstwowej ochrony, znanym jako „defense in depth”. Pierwszą i fundamentalną zasadą jest zasada najmniejszych uprawnień, która zakłada, że każdy użytkownik powinien mieć dostęp tylko do tych zasobów, które są niezbędne do wykonywania jego obowiązków służbowych. Takie podejście znacząco redukuje ryzyko nieautoryzowanego dostępu do wrażliwych danych oraz minimalizuje potencjalne szkody w przypadku kompromitacji konta użytkownika. Druga istotna zasada dotyczy segmentacji i separacji obowiązków. W praktyce oznacza to, że krytyczne procesy powinny być podzielone między różne osoby lub działy, co zapobiega nadużyciom i błędom. Na przykład, osoba zatwierdzająca transakcje finansowe nie powinna być jednocześnie osobą je wykonującą. Taka separacja obowiązków stanowi skuteczny mechanizm kontrolny i redukuje ryzyko fraudów. Zasada głębokiej ochrony (defense in depth) stanowi trzeci filar bezpieczeństwa informacji. Zgodnie z nią, ochrona zasobów informacyjnych powinna być realizowana na wielu poziomach, poczynając od zabezpieczeń fizycznych, poprzez kontrole dostępu logicznego, aż po monitoring i audyt. Każda warstwa bezpieczeństwa powinna być niezależna od pozostałych, dzięki czemu przełamanie jednej z nich nie prowadzi automatycznie do kompromitacji całego systemu” (Godula, 2026).

Bezpieczeństwo informacji jest kwestią niezwykle ważną w kontekście każdego działania, dlatego organizacje powinny zadbać nie tylko o procedury i polityki bezpieczeństwa, ale też o systematyczne audyty. Audyt bezpieczeństwa informacji to systematyczny i kompleksowy przegląd procedur i polityki bezpieczeństwa; wiąże się z realną i wymierną oceną, czy organizacja stosuje skuteczne działania prewencyjne chroniące m.in. przed wyciekiem danych i cyberatakami. Działania audytorskie, a więc prowadzenie audytu bezpieczeństwa informacji, to systematyczny proces oceny i przeglądu procedur, polityk i systemów informatycznych organizacji w celu weryfikacji ich skuteczności i zgodności z normami i przepisami.

Rodzaje audytów bezpieczeństwa

Utrzymanie wysokich standardów funkcjonowania organizacji jest kluczowe dla osiągnięcia sukcesu. Jednym z najważniejszych narzędzi wspierających ten proces jest audyt – systematyczne badanie i analiza

działań organizacji, mające na celu identyfikację obszarów wymagających poprawy oraz wdrażanie skutecznych działań korygujących. Audyty, zarówno wewnętrzne, jak i operacyjne, odgrywają istotną rolę w zarządzaniu ryzykiem, zapewnieniu zgodności z przepisami wewnętrznymi organizacji i obowiązującymi standardami (Hotiuk, 2024). Audyt bazuje na specyficznych działaniach, które mają na celu ocenić dany system, proces, projekt lub organizację. Przebieg audytu determinuje również jego rodzaj. Rodzaje audytów różnią się zakresem i celem, jednak każde badanie ma na celu analizę procesów oraz zapewnienie działań wspierających poprawę funkcjonowania organizacji w praktyce. Jak już wspomniano we wstępie audyty dzielą się na wewnętrzne (pierwszej strony) i zewnętrzne (drugiej i trzeciej strony). Zasadnicza różnica między nimi polega przede wszystkim na podmiocie, który je przeprowadza, a także celowi stojącemu za tymi działaniami. Jeśli chodzi o przedmiot audytu, jest on badany w odniesieniu do konkretnych standardów, przepisów prawnych, wzorców i norm. Jednym z kryteriów podziału audytów jest podmiot, który je przeprowadza. W tym zakresie wyróżnia się trzy podstawowe sposoby audytowania: audyt pierwszej strony (wewnętrzny), audyt drugiej strony oraz audyt trzeciej strony (z czego ostatni z opisanych poniżej – tj. audyt trzeciej strony – jest zdecydowanie najrzadszy). Przebieg audytu determinuje również jego rodzaj. Każdy z nich jest inny i ma określony własny cel. Jak już wspomniano wcześniej, audyty dzielą się na wewnętrzne (pierwszej strony) i zewnętrzne (drugiej i trzeciej strony). Zasadnicza różnica między nimi polega przede wszystkim na podmiocie, który je przeprowadza, a także celowi stojącemu za tymi działaniami.

Tabela 1. Rodzaje audytów bezpieczeństwa

Audyt pierwszej strony (audyt wewnętrzny)	Audyt wewnętrzny jest jednym z najlepszych narzędzi służących do ciągłego doskonalenia organizacji. Jest audytem wewnętrznym i jest prowadzony przez samą organizację lub w jej imieniu. Podczas tych działań ocenia się wdrożony system pod kątem prawidłowości i poprawności działania w chwili kontroli. Zgodnie z przyjętą zasadą, audytorzy nie mogą audytować obszarów, za które są odpowiedzialni. Audyt wewnętrzny jest audytem cyklicznym obejmującym określony obszar lub całą organizację.
Audyt drugiej strony (audyt zewnętrzny)	Audyt koncentruje się na badaniu systemu zarządzania przez klienta lub zainteresowaną instytucję. Takie audyty są już wykonywane przez certyfikowanych audytorów bezpieczeństwa, którzy mogą być zarówno wewnątrz organizacji, a także z zewnątrz. Przeprowadzenie takiego audytu musi być poparte pisemnym porozumieniem, np. umową.
Audyt trzeciej strony (audyt zewnętrzny)	Audyt jest przeprowadzany dla celów certyfikacji lub akredytacji, jak również dla celów prawnych i regulacyjnych. Audyty te są przeprowadzane przez niezależne organizacje audytorskie, które weryfikują poprawność funkcjonowania systemów do istniejących przepisów.
Audyt połączony (zintegrowany)	Audyt przeprowadzany wspólnie u jednego audytowanego w kontekście dwóch lub więcej systemów zarządzania.
Audyt wspólny	Audyt przeprowadzany u jednego audytowanego przez dwie lub więcej organizacji audytorskich.

Źródło: Jurkiewicz P. (2023). *Jak audyt bezpieczeństwa wygląda w praktyce?* Pobrano z: <https://www.doering-partnerzy.pl/jak-audit-bezpieczenstwa-wyglada--w-praktyce/> (dostęp: 20.09.2025).

Audyt wewnętrzny (określany audytem pierwszej strony lub audyt wewnętrzny procesu) – w większości międzynarodowych standardów, w tym w normach z rodziny ISO, audyty wewnętrzne traktowane są jako ważna część procesu ciągłego doskonalenia organizacji, ponieważ umożliwiają one monitorowanie i przeglądanie wydajności procesów. Audyty wewnętrzne dają organizacji możliwość zidentyfikowania potencjalnego ryzyka i luk w systemie oraz zaprojektowania działań naprawczych, zanim zaczną generować poważne koszty dla organizacji. Pomagają również śledzić i dokumentować ewentualne zmiany. Dostarcza wiedzę czy wszystko działa zgodnie z założeniami. Najczęściej przeprowadzany jest przez osoby

na stałe zatrudnione w danym podmiocie – funkcjonują w ramach jej struktury, choć jednocześnie zachowują odpowiednią niezależność organizacyjną. Rzadziej są to audytorzy, którym zleca się tego typu czynność np. na podstawie umowy zlecenia. Jak wskazuje definicja stworzona przez The Institute of Internal Auditors (IIA – Instytut Audytorów Wewnętrznych), to niezależna, obiektywna działalność o charakterze doradczym, prowadzona w celu wniesienia do organizacji wartości dodanej i usprawnienia jej funkcjonowania. Zgodnie z definicją Instytutu Audytorów Wewnętrznych (IIA), audyt wewnętrzny (Instytut Audytorów Wewnętrznych IIA Polska, b.d.) jest działalnością niezależną i obiektywną, której celem jest przysporzenie wartości i usprawnienie działalności operacyjnej organizacji. Polega on na systematycznej i dokonywanej w uporządkowany sposób ocenie procesów zarządzania ryzykiem, kontroli i ładu organizacyjnego, przyczyniając się do poprawy ich działania. Audyt wewnętrzny stanowi kluczowy element systemu kontroli wewnętrznej organizacji, dostarczając kierownictwu cennych informacji i rekomendacji. Generalnie pełni zatem rolę przede wszystkim wspierającą – ma ułatwiać realizowanie celów danej organizacji, podwyższać efektywność działania zatrudnionych w niej osób, ułatwiać wykonywanie ich obowiązków, identyfikować ewentualne ryzyka i dawać wskazówki w zakresie przygotowania odpowiednich procesów zarządzania ryzykiem i wskazywać możliwe sposoby ich minimalizowania itp. Co więcej, audyt wewnętrzny został zdefiniowany także w Dziale VI. ustawy o finansach publicznych i dotyczy audytowania oraz koordynacji owych audytów w jednostkach sektora finansów publicznych. Art. 272 wskazuje, że: „Audyty wewnętrzne są działalnością niezależną i obiektywną, której celem jest wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze”. Istnienie odpowiednich komórek audytu wewnętrznego jest w tym przypadku obowiązkowe, co ma ogromne znaczenie dla ochrony interesów społecznych. Audyt wewnętrzny dostarcza wiedzę z pierwszej ręki wewnątrz czy wszystko działa zgodnie z założeniami. Często bywa tak, że oceny wyników audytu interpretowana jest jak wyrocznia. Zgodnie z założeniami audyt wewnętrzny ma służyć jako narzędzie wspomagające proces rozwoju organizacji wg wewnętrznych zasad zarządzania panujących w organizacji (Lean Partner, b.d.). Podstawą audytu jest weryfikacja systemu zarządzania, nie ocena pracy ludzi i doszukiwanie się niezgodności. Audyt

wewnętrzny przynosi organizacji wiele korzyści. Przede wszystkim przyczynia się do poprawy efektywności i skuteczności operacji poprzez identyfikację obszarów wymagających usprawnień. Wzmacnia system kontroli wewnętrznej, co pomaga w minimalizacji ryzyka błędów i nadużyć. Audyt wewnętrzny wspiera również lepsze zarządzanie ryzykiem, pomagając organizacji w identyfikacji i ocenie potencjalnych zagrożeń. Ponadto, audyt wewnętrzny przyczynia się do zwiększenia zgodności z przepisami i regulacjami, co jest szczególnie istotne w dzisiejszym złożonym środowisku prawnym. Wspiera osiąganie celów strategicznych organizacji poprzez dostarczanie informacji niezbędnych do podejmowania decyzji. Wreszcie, audyt wewnętrzny dostarcza obiektywnych informacji zarządowi i kierownictwu, co pomaga w podejmowaniu świadomych decyzji strategicznych (EITT, b.d.). Audyt wewnętrzny jest cennym narzędziem wspierającym organizację w osiąganiu jej celów i poprawie efektywności działania. Poprzez systematyczną ocenę procesów i dostarczanie obiektywnych informacji, audyt wewnętrzny przyczynia się do tworzenia wartości dodanej i usprawnienia działalności operacyjnej organizacji.

Audyt zewnętrzny to niezależna ocena, przeprowadzana przez podmiot niebędący częścią audytowanej organizacji. Audyt zewnętrzny przeprowadzany jest przez niezależnych ekspertów, niemających bezpośredniego związku z organizacją. Audyt zewnętrzny może zostać przeprowadzony zarówno przez drugą, jak i trzecią stronę. Organizacja nie korzysta wówczas z własnych zasobów, ale musi zaangażować niezależnych ekspertów, gwarantujących bezstronną i obiektywną perspektywę. W obu przypadkach cel stanowi przede wszystkim ocena skuteczności systemu zarządzania oraz potwierdzenie zgodności z wymaganiami danej normy ISO. Audyt zewnętrzny - przeprowadzają go podmioty niezależne od danej organizacji, inaczej określany audytem drugiej strony. Osoba audytująca musi jednak posiadać niezbędne do tego kompetencje i być uprawnionym audytorem (wewnętrznym lub zewnętrznym). Najczęściej są to wyspecjalizowane firmy konsultingowe lub audytorskie, które zatrudniają audytorów i rewidentów w pełni przygotowanych do auditingu (posiadających odpowiednie uprawnienia). W tym przypadku kluczowa jest ocena funkcjonowania wybranych jednostek pod względem finansowym, w przeciwieństwie do audytu wewnętrznego, który często obejmuje także obszary niefinansowe.

Audyt trzeciej strony – to szczególna forma audytu zewnętrznego (audyt certyfikacyjny). Audytorzy są bowiem zupełnie niezależni od podmiotu, który analizują. Są to np. jednostki certyfikujące (jeżeli dany podmiot chce uzyskać akredytowany certyfikat ISO, poddawanie się tego typu audytom jest obowiązkowe).

Dążenie do ciągłego doskonalenia organizacji pracy i funkcjonowania organizacji stanowi kluczowy element rozwoju. Należy pamiętać, że wdrożenie systemu zarządzania ISO to jeden z etapów złożonego procesu. Aby podjęte działania były zgodne z wymaganiami danej normy ISO, konieczne jest regularne przeprowadzanie audytów. Każdy audyt, zarówno pierwszej, drugiej, jak i trzeciej strony może przynieść organizacji wiele korzyści. Audyt wewnętrzny pozwala na dalsze doskonalenie wdrożonego systemu zarządzania poprzez identyfikację obszarów wymagających poprawy w celu podniesienia efektywności i standardów w danej organizacji. Przeprowadzenie audytów zewnętrznych, zarówno drugiej, jak i trzeciej strony pomaga w skutecznym budowaniu profesjonalnego i wiarygodnego wizerunku (CeCert, 2024). Zasadniczo mówimy o trzech rodzajach audytów: audyt pierwszej strony (audyt wewnętrzny), audyt drugiej strony (audyt klienta u dostawcy) i audyt trzeciej strony (audyt wykonywany przez niezależną organizację, np. audyt jednostki certyfikacyjnej). Wszystkie ww. typy audytów mają elementy wspólne, ale też się różnią, ponieważ pełnią nieco inne role w systemie.

Tabela 2. Różnice między audytami pierwszej, drugiej i trzeciej strony

Proces audytu	Audyt pierwszej strony	Audyt drugiej strony	Audyt trzeciej strony
Cel audytu	Ocena stopnia spełnienia wymagań danej normy i wymagań własnych organizacji oraz skuteczności systemu.	Ocena stopnia spełnienia wymagań przez dostawcę.	Ocena stopnia spełnienia wymagań danej normy w odniesieniu do zakresu i kryteriów jego certyfikacji, nadzoru lub recertyfikacji.
Zakres audytu	Konkretny obszar lub proces w zakresie systemu.	Procesy, działania, usługi realizowane przez zewnętrznego dostawcę.	Udokumentowany zakres systemu zarządzania w stosunku do wymogów danej normy.

Proces audytu	Audyt pierwszej strony	Audyt drugiej strony	Audyt trzeciej strony
Kryteria	Punkty normy stanowiącej podstawę systemu, realizowane w danym obszarze/ procesie oraz konkretna dokumentacja wspierająca działania w obszarze lub proces	Dokument zawierający wymagania organizacji (np. umowa, specyfikacji, zamówień, zleceń, itp.) na podstawie których dostawca realizuje zlecony proces czy usługę	Norma, która stanowi podstawę danego systemu oraz dokumentacja systemu zarządzania
Długość trwania audytu	Jest ustalany przez audytora i zależy od stopnia skomplikowania procesu, jego znaczenia w systemie i poziomu ryzyk	Jest ustalany przez audytora i wynika z zakresu zleconych działań, procesów lub realizowanych usług	Jest wyliczany przez jednostkę certyfikującą na podstawie określonych kryteriów i zasadniczo jest nienegocjowalny
Kompetencje audytora	Ustala organizacja wg własnych kryteriów z uwzględnieniem wiedzy i umiejętności niezbędnych do prowadzenia audytu wewnątrz organizacji	Ustala organizacja wg własnych kryteriów z uwzględnieniem wiedzy i umiejętności niezbędnych do prowadzenia audytu u konkretnego dostawcy	Wynikają z normy ISO 17021 i innych dokumentów obowiązujących akredytowaną jednostkę certyfikacyjną

Źródło: opracowanie własne na podstawie Biarda, M. (2022), *Rola audytu w systemach zarządzania*. Pobrano z: <https://jakoscbezretuszu.pl/rola-audytu-w-systemach-zarzadzania/> (dostęp: 12.02.2026).

Regularne przeprowadzanie audytów bezpieczeństwa jest kluczowe dla utrzymania wysokiego poziomu ochrony danych i systemów informatycznych, co pomaga organizacjom przeciwdziałać potencjalnym zagrożeniom oraz reagować na incydenty bezpieczeństwa w odpowiedni sposób. Audyt powinna wykonać jednostka zewnętrzna, aby zyskać gwarancję rzetelnej, bezstronnej i miarodajnej oceny. Audyty z reguły powinny być przeprowadzane przez osoby posiadające doświadczenie i kompetencje poparte stosowanymi certyfikatami. Audyt wykonują specjalnie przygotowani do tego audytorzy, którzy w swoim działaniu m.in. muszą kierować się zasadami: rzetelności, uczciwości, zgodności z etyką, należytej staranności, niezależności, poufności i wnioskowaniu w oparciu o konkretne dowody.

Jakość audytu bezpieczeństwa informacji

Jakość audytu bezpieczeństwa informacji (np. wg ISO/IEC 27001) jest bezpośrednio i nierozdzielnie związana z kompetencjami, doświadczeniem oraz postawą audytora. Audytor jest ekspertem, którego rzetelność i umiejętności definiują wartość dodaną dla organizacji. Audytor bezpieczeństwa informacji to specjalista przeprowadzający systematyczne oceny systemów, procesów i procedur organizacji w celu identyfikacji zagrożeń, luk w zabezpieczeniach i niezgodności, zapewniając ochronę danych i ciągłość działania, często w oparciu o normy takie jak ISO/IEC 27001. Jego rola polega na weryfikacji infrastruktury IT, procedur, polityk i kompetencji personelu, a następnie rekomendowaniu działań naprawczych i usprawnień, co pomaga spełniać wymogi prawne, budować zaufanie i minimalizować ryzyko. Audytor bezpieczeństwa informacji to osoba, która posiada odpowiednie kwalifikacje i doświadczenie do przeprowadzania audytów systemów zarządzania bezpieczeństwem informacji. Audytor ocenia, czy organizacja skutecznie chroni swoje dane oraz czy spełnia wymagania określone przez międzynarodowe standardy, takie jak ISO/IEC 27001. Jego zadaniem jest również identyfikacja luk w zabezpieczeniach oraz rekomendowanie działań mających na celu ich eliminację. Jeśli chodzi o audytorów wewnętrznych systemów zarządzania, szczególnie podkreśla się konieczność znajomości przez nich struktury i wymagań wynikających z normy ISO 9001, zaś audytorzy systemu zarządzania bezpieczeństwem informacji – normy ISO/IEC 27001. Do przeprowadzania audytów przygotowują przede wszystkim odpowiednie szkolenia, które prowadzone są przez certyfikowane jednostki, działające na podstawie przyjętych standardów zawodowych.

Rola audytora bezpieczeństwa informacji obejmuje szereg kluczowych obowiązków. Audytor jest odpowiedzialny za planowanie i przeprowadzanie audytów bezpieczeństwa, co obejmuje analizę systemów informacyjnych, ocenę procedur bezpieczeństwa oraz identyfikację potencjalnych zagrożeń. Audytor musi również dokumentować wyniki audytu i przedstawiać je kierownictwu organizacji, dostarczając rekomendacje dotyczące usprawnień. Jego obowiązki obejmują także monitorowanie wdrażania zaleceń oraz zapewnienie, że organizacja spełnia wszystkie wymagania regulacyjne i normatywne.

Audytor bezpieczeństwa informacji odgrywa kluczową rolę w systemie zarządzania bezpieczeństwem informacji. Jego praca pomaga

organizacjom w identyfikacji i eliminacji słabości w systemach zabezpieczeń, co jest niezbędne do ochrony danych i zgodności z regulacjami prawnymi. Audytor dostarcza kierownictwu obiektywnych informacji na temat stanu bezpieczeństwa informacji, co pozwala na podejmowanie świadomych decyzji strategicznych. Dzięki jego rekomendacjom organizacje mogą poprawić swoje procedury bezpieczeństwa i zminimalizować ryzyko związane z zagrożeniami cybernetycznymi.

Przewagą organizacji, w strukturach której funkcjonuje audytor wewnętrzny, jest możliwość nieustannego kontrolowania zachodzących procesów. W pewnym sensie audyt trwa tam przez cały rok, dzięki czemu daje też szanse na szybkie zauważenie pojawiających się trudności i równie szybko im zaradzenia. Co ważne, specjaliści kierują się w trakcie audytowania przepisami prawa, zarówno krajowego, jak i międzynarodowego (np. Unii Europejskiej), przepisami wewnętrznymi organizacji, określonymi standardami, listami kontrolnymi czy normami. Audytor powinien mieć wiedzę o procesach występujących w organizacji, procedurach obowiązujących w organizacji, a dodatkowo wiedzę specjalistyczną np. z zakresu IT, bezpieczeństwa informacji, stosowanych zabezpieczeniach i pojawiających się zagrożeń. Powinien znać również podstawowe wymagania prawne z danego obszaru. W zależności od wymagań audyt przeprowadzany jest przez jednego audytora lub grupę audytorów. Jeżeli audyt przeprowadzany jest przez zespół audytorów, w takim przypadku należy wskazać audytora wiodącego. Jest to osoba prowadząca audyt, na którym oparta jest cała odpowiedzialność za prawidłowe przeprowadzenia tego procesu. To on m.in. określa plan audytu, wytycza zakres czynności audytu w danej organizacji, a na koniec tworzy raport z audytu. Jeżeli przeprowadzamy audyt bezpieczeństwa informacji dobrze jest, aby w zespole byli również choć jeden audytor IT (Jurkiewicz, 2023). Audyt jest tak dobry, jak doświadczenie i wiedza członków zespołu audytorskiego; dlatego, aby audyt przebiegł pomyślnie, członkowie zespołu audytorskiego powinni być starannie wybierani i odpowiednio przeszkoleni. Cechy audytora wewnętrznego zostały określone między innymi w normie ISO 19011. Zawiera ona wytyczne dotyczące cech osobowości, charakterystycznych dla tego zawodu (Przybylska, Rydzak, Trębecki, 2021, s.16). Katalog przymiotów audytorskich wg ISO 19011 obejmuje bycie (Global Cert, 2023):

- Profesjonalizm: Audytor będzie posiadał cechy osobiste, takie jak wiarygodność, uczciwość i rzetelność, i będzie dostarczał rzetelnych informacji i wyników dotyczących jednostki, którą audytuje. Ponadto osoba ta podejmuje się działań audytowych tylko, gdy ma do tego kompetencje i pozostaje bezstronnym,
- Otwartość: Audytor będzie chętny słuchać, uczyć się i akceptować nowe pomysły oraz odzwierciedlać je w sytuacjach lub wymaganiach. Czasami audytor może napotkać nowe podejścia lub opinie. Audytor, pozostając obiektywnym musi mieć zdolność oceny i akceptacji różnych punktów widzenia, o ile spełniają one wymagania,
- Dyplomatyczność: Audytor będzie uprzejmy i świadomy swojej roli; audytor pełni funkcję reprezentacyjną, a więc przedstawiciela danej organizacji,
- Obserwator: Audytor będzie miał zdolność rozpoznawania i oceniania tego, co widzi, oraz rozumienia i interpretowania zdarzeń bez głębokiego przesłuchania,
- Perspektywa: Audytor będzie miał zdolność oceny sytuacji wykraczających poza wygląd osoby, z systematycznym poglądem na rzeczy i będzie miał zdolność zrozumienia konsekwencji organizacyjnych dowodów, które znajdzie,
- Wszechstronność: Audytor będzie miał zdolność do mobilizacji z jednej sytuacji do drugiej bez utraty kierunku. W jednej chwili audytor może audytować jedno pole; w następnej może to być inne. Audytor musi być w stanie pozostać skupionym,
- Wytrwałość: Audytor musi być wytrwały w swoich celach, tak, aby gdy zada pytanie, musiał otrzymać na nie odpowiedź i nie był rozpraszany przez zakłócenia lub zakłócenia. Zaleca się, aby dowód z audytu był weryfikowalny, dlatego próba uzyskania jak największej ilości informacji i dowodów jest jedynym słusznym podejściem,
- Niezależność: Audytor musi mieć własne zdanie na różne tematy, nie będzie pod wpływem otoczenia i będzie wolny od konfliktu interesów. Zaleca się, aby audytorzy byli niezależni od działań poddanych audytowi (w ramach możliwości),

- Decyzyjność: Audytor musi być gotowy podejmować decyzje, nawet jeśli są trudne lub nie zadowolą audytowanego,
- Poufność: Zaleca się, aby audytorzy wykazywali się dyskrecją w użyciu i ochronie informacji, do których otrzymują dostęp w wyniku wykonywania swoich obowiązków. Informacje audytowe nie mogą być wykorzystywane dla osobistych korzyści przez audytora lub klienta audytu.

Zakres umiejętności wymaganych od liderów audytu wewnętrznego stale się poszerza. Muszą oni posiadać kompetencje techniczne i strategiczne, aby móc współpracować z interesariuszami. Muszą być również skutecznymi liderami i strategami z dobrą znajomością organizacji. Audytorzy wewnętrzni odgrywają kluczową rolę w zapewnianiu właściwego ładu korporacyjnego, zarządzania ryzykiem i kontroli w organizacjach. Wraz z rozwojem funkcji audytu wewnętrznego, zmienia się również zakres umiejętności wymaganych od lidera audytu wewnętrznego. 10 najważniejszych cech wyróżniających wybitnych liderów audytu wewnętrznego (Highspring, 2025).

Wiarygodny: wybitni liderzy audytu wewnętrznego muszą być w stanie budować i utrzymywać wiarygodność na wysokim szczeblu w organizacji. Będą musieli konfrontować się z dyrektorami generalnymi i innymi interesariuszami najwyższego szczebla, co wymaga doskonałych umiejętności komunikacyjnych i umiejętności kwestionowania poglądów kadry kierowniczej wyższego szczebla. W tym celu muszą wykorzystywać dane do opracowania planu strategicznego, który jest zgodny z celami organizacji i zawiera konkretne kroki prowadzące do osiągnięcia sukcesu. Dobrze sporządzone raporty z audytu pomagają umocnić wiarygodność audytora wewnętrznego, gwarantując, że jego ustalenia i zalecenia będą traktowane poważnie i wdrażane przez kadrę kierowniczą wyższego szczebla.

Godny zaufania: budowanie zaufania jest kluczowe dla liderów audytu wewnętrznego, którzy muszą być w stanie budować i utrzymywać zaufanie interesariuszy na wszystkich szczeblach, w tym kierownictwa, pracowników i interesariuszy zewnętrznych. Dobry dyrektor audytu wewnętrznego potrafi angażować i wpływać na interesariuszy w całej organizacji, jednocześnie budując wysoki poziom zaufania i szacunku. Chociaż budowanie tych relacji może być czasochłonne, korzyści są niezaprzeczalne.

Ujmujący: wiarygodność i budowanie zaufania idą w parze, przyczyniając się do powstania trzeciej cechy, która staje się kluczowa dla liderów audytu wewnętrznego: zaangażowania interesariuszy. Budowanie relacji opartych na współpracy z interesariuszami jest koniecznością, a skuteczni audytorzy stosują skuteczną komunikację, aby ograniczyć opór w procesie audytu, promować lepsze zrozumienie wartości audytu wewnętrznego dla organizacji oraz przyspieszyć udostępnianie informacji w odpowiedzi na wnioski audytowe. W tym obszarze zbudowanie silnego zespołu audytu wewnętrznego może usprawnić współpracę z interesariuszami i zapewnić sprawny i efektywny proces audytu.

Technicznie uzdolniony: chociaż pracodawcy kładą większy nacisk na umiejętności miękkie, kompetencje techniczne pozostają fundamentalne dla kierowników stanowisk audytorskich. Kluczowi interesariusze oczekują najwyższego poziomu kompetencji technicznych w zakresie kontroli wewnętrznej, a wszyscy audytorzy wewnętrzeni muszą znać szereg platform analityki danych, wykorzystując je do zwiększania wartości organizacji w ramach działań audytu wewnętrznego. Inne kwestie, takie jak audyty zgodności, różnią się w zależności od branży. Na przykład świadomość regulacyjna jest szczególnie ważna w sektorze usług finansowych i bankowości, dlatego kluczowe jest posiadanie inwentarza umiejętności i modelu talentów, który odpowiada ryzyku i potrzebom organizacji.

Strategiczny: chociaż audyt stanowi trzecią linię obrony, organizacje oczekują więcej od swoich obszarów ładu korporacyjnego, co często wiąże się z coraz bardziej aktywną odpowiedzialnością w myśleniu strategicznym. Liderzy audytu wewnętrznego muszą wdrażać i wykorzystywać nowe technologie, aby realizować swoje wytyczne strategiczne, proaktywnie rozwiązując potencjalne problemy, a nie tylko na nie reagując. Ten poziom planowania jest niezbędny nie tylko w przypadku audytów wewnętrznych, ale także zewnętrznych, aby pomóc organizacjom identyfikować ryzyka i odkrywać obszary wymagające poprawy.

Nastawiony na biznes: liderzy audytu wewnętrznego muszą posiadać dogłębną wiedzę na temat działalności operacyjnej organizacji, procesów sprawozdawczości finansowej oraz branży. Wybitni liderzy audytu wewnętrznego powinni również posiadać silną orientację biznesową i umieć wykorzystać swoją wiedzę do identyfikacji ryzyka i tworzenia skutecznych mechanizmów kontroli. Powinni rozpoznawać kluczowe elementy sukcesu

swojej organizacji, zwiększając wartość dodaną poprzez budowanie działu audytu wewnętrznego w oparciu o te zasady.

Zrównoważony: oprócz tradycyjnych umiejętności audytorskich, liderzy audytu wewnętrznego o specjalistycznych kompetencjach cieszą się dużym zainteresowaniem. Banki i instytucje finansowe chętnie zatrudniają audytorów posiadających specjalistyczną wiedzę regulacyjną w zakresie płynności, kredytów i zarządzania ryzykiem. Znajomość systemów rachunkowości finansowej i sprawozdawczości, przepisów o zamówieniach publicznych w sektorze obronnym oraz wymogów systemów zarządzania kosztami ma kluczowe znaczenie dla wszechstronnego audytora, a osoby posiadające taką wiedzę są bardzo poszukiwane. Specjalistyczne umiejętności audytu wewnętrznego, na przykład w zakresie bezpieczeństwa danych, są coraz bardziej cenione podczas przeprowadzania audytów finansowych w branżach o rygorystycznych wymogach regulacyjnych.

Innowacyjny: chociaż rodzaj wymaganych umiejętności przywódczych może się różnić w zależności od organizacji, skuteczne przywództwo wymaga złożonego, ewoluującego zestawu umiejętności. Najlepsi liderzy nieustannie poszukują nowych pomysłów i sposobów na zwiększenie efektywności poprzez innowacje. W rozwijaniu umiejętności przywódczych, ciągle doskonalenie i ocena naprawdę się opłacają.

Zręczny: krajobraz audytu wewnętrznego nabiera tempa, a liderzy muszą być gotowi i zdolni do wprowadzania zmian w swoich rocznych planach audytu w obliczu nieoczekiwanych zmian warunków rynkowych. Szybkie myślenie i rozwiązywanie problemów to kluczowe umiejętności leżące u podstaw audytu wewnętrznego, a najlepsi specjaliści od rozwiązywania problemów będą wykorzystywać kreatywność i innowacyjność w rozwiązywaniu złożonych problemów. Cechy te są szczególnie ważne w audycie operacyjnym, gdzie nacisk kładzie się na ocenę efektywności wdrożonych procesów, polityk, procedur i systemów. Wraz z ciągłą ewolucją wymagań regulacyjnych, procesów i technologii, audytorzy muszą podchodzić do świadczenia usług audytorskich i doradczych z perspektywą, zachowując otwartość i gotowość do angażowania się w odpowiedni poziom ryzyka.

Wpływowy: kultura organizacji ma coraz większe znaczenie dla ładu korporacyjnego, a audyt wewnętrzny nie jest wyjątkiem. Liderzy audytu wewnętrznego stanowią kluczowy wzór do naśladowania w utrzymywaniu zespołów zarządzających na właściwym kursie. Zapewniając obiektywne

zapewnienie lub bezstronną ocenę, liderzy audytu wewnętrznego mogą wpływać na kulturę przejrzystości i ciągłego doskonalenia. Zamiast unikać zmian, najlepsi liderzy audytu wewnętrznego starają się je inspirować i tworzyć atmosferę, w której ludzie chętnie wdrażają innowacyjne pomysły.

Profesjonalni audytorzy, na których można polegać: jeśli interesariusze uznają liderów audytu wewnętrznego za wysoce skutecznych w tych cechach, wówczas lider audytu wewnętrznego, jako zaufany doradca, wnosi znaczącą wartość dodaną do organizacji. Liderzy audytu wewnętrznego budują zaufanie poprzez konsekwentną współpracę z interesariuszami na wszystkich szczeblach organizacji i transparentną komunikację. Skuteczna komunikacja jest jedną z pięciu najważniejszych kompetencji zawodowych wymaganych w środowisku audytorów wewnętrznych. Zapewniając obiektywne zapewnienie i przedstawiając jasne, uzasadnione rekomendacje, pokazują, że mają na uwadze dobro organizacji. Z czasem te działania budują wysoki poziom szacunku i zaufania, zwłaszcza wśród kadry kierowniczej wyższego szczebla, pomagając liderom audytu wewnętrznego wpływać na decyzje organizacji i wprowadzać pozytywne zmiany. Skuteczni liderzy audytu wewnętrznego potrzebują połączenia wiedzy technicznej, myślenia strategicznego i silnych umiejętności przywódczych. Często wiąże się to z budowaniem wiarygodności, budowaniem zaufania i angażowaniem interesariuszy w całej organizacji poprzez skuteczne umiejętności komunikacyjne. Powinni również korzystać z nowych technologii, aby wyprzedzać potencjalne zagrożenia i szanse, dostarczać cennych spostrzeżeń i pomagać w kształtowaniu strategicznego kierunku organizacji (Highspring, 2025). Audytor rozumie sytuację w jakiej się znajduje, uwzględnia wszelkie niuanse, emanuje kulturą osobistą i pewnością. W praktyce audytor ma do czynienia z różnymi charakterami i postawami audytowanego. Musi zatem być przygotowany w różne scenariusze, zwłaszcza podczas rozmów, które są przecież jednym z najważniejszych źródeł zbierania informacji (Global Cert, 2023). Praca audytora bezpieczeństwa informacji wiąże się z wieloma wyzwaniami. Jednym z nich jest konieczność nadążania za szybko zmieniającym się krajobrazem zagrożeń cybernetycznych, co wymaga ciągłego doskonalenia wiedzy i umiejętności. Audytorzy muszą również radzić sobie z złożonością systemów informatycznych oraz zapewniać, że ich oceny są obiektywne i niezależne. Najlepsze praktyki w pracy audytora obejmują regularne szkolenia i aktualizację wiedzy, stosowanie międzynarodowych

standardów i norm oraz efektywną komunikację z kierownictwem organizacji. Ważne jest również, aby audytorzy angażowali różne działy organizacji w proces audytu, co pozwala na uzyskanie pełniejszego obrazu stanu bezpieczeństwa. Dokumentowanie wyników audytu i monitorowanie wdrażania zaleceń to kluczowe elementy, które pomagają w zapewnieniu skuteczności działań audytowych i poprawie bezpieczeństwa informacji w organizacji (EITT, b.d.). Chambers i McDonald zwracają uwagę, że wraz z rozwojem audytu zmieniają się oczekiwania, co do kwalifikacji i kompetencji (zwanych atrybutami) audytorów. Umiejętności techniczne pozostają absolutnie niezbędne, ale same w sobie nie są już wystarczające. Skuteczny „audytor przyszłości”, obok umiejętności technicznych musi posiadać szeroki zakres nietechnicznych atrybutów. Siedem najbardziej pożądanых atrybutów skutecznego audytora, zidentyfikowanych przez Chambersa i McDoalda to: umiejętność skutecznego komunikowania się, partnerstwo, umiejętność pracy zespołowej, globalny sposób myślenia, budowane relacje, ciągle podnoszenie kwalifikacji, uczciwość (Przybylska i in., 2021, s. 19).

Audytor bezpieczeństwa informacji to specjalista odpowiedzialny za przeprowadzanie audytów mających na celu ocenę i zapewnienie skuteczności systemów zarządzania bezpieczeństwem informacji w organizacji. Jego rola jest kluczowa w identyfikacji potencjalnych zagrożeń, ocenie zgodności z normami oraz rekomendowaniu działań naprawczych. Audytor, który dobrze rozumie kontekst organizacji, podnosi jej cyberbezpieczeństwo. Wysoka jakość audytu skutkuje lepszym zarządzaniem ryzykiem, wyższą poufnością, integralnością i dostępnością informacji.

Podstawowe zasady audytowania

Audyt bezpieczeństwa informacji to systematyczna ocena systemów, procedur i praktyk organizacji w celu zidentyfikowania potencjalnych zagrożeń, luk w zabezpieczeniach oraz niezgodności z politykami i przepisami, aby zapewnić poufność, integralność i dostępność danych. Wynikiem audytu jest raport z rekomendacjami, a jego celem jest zwiększenie odporności organizacji na cyberataki i zapewnienie bezpieczeństwa danych, co jest kluczowe dla zgodności z prawem i utrzymania zaufania. Proces ten bada kilka kluczowych obszarów:

- Polityki i procedury: analiza dokumentacji organizacyjnej dotyczącej bezpieczeństwa informacji, w tym procedur zarządzania danymi, reagowania na incydenty i zasad postępowania z poufnymi informacjami,
- Infrastruktura techniczna: ocena zabezpieczeń systemów informatycznych, takich jak sieci, serwery, oprogramowanie antywirusowe, mechanizmy szyfrowania i metody uwierzytelniania, często z wykorzystaniem testów penetracyjnych,
- Praktyki pracowników: weryfikacja czy pracownicy stosują odpowiednie procedury, są świadomi zagrożeń i przestrzegają polityk bezpieczeństwa, a także ocena poziomu ich świadomości poprzez ewentualne szkolenia,
- Zgodność: sprawdzenie czy organizacja przestrzega obowiązujących przepisów prawa (np. RODO), norm branżowych (np. ISO/IEC 27001) oraz wytycznych organów nadzoru.

Podczas audytu bezpieczeństwa informacji sprawdzane są między innymi (Klichowski, b.d.):

- zgodność z obowiązującymi normami,
- bezpieczeństwo procesów związanych z przepływem informacji, infrastruktury i oprogramowania,
- bezpieczeństwo informacji w relacjach z dostawcami,
- bezpieczeństwo systemów informacyjnych,
- zarządzanie aktywami,
- zarządzanie ciągłością działania,
- kontrola dostępu,
- bezpieczeństwo komunikacji.

Częstotliwość audytu powinna być podyktowana charakterystyką działalności organizacji. Im jest ona bardziej ryzykowna i „wyeksponowana”, tym badanie należy przeprowadzać częściej. Audyty bezpieczeństwa przeprowadza się zgodnie z oczekiwaniami i potrzebami organizacji, jak również wymaganiami prawnymi. Dobrą praktyką jest przeprowadzenie audytu bezpieczeństwa co najmniej raz do roku. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560), (Ministerstwo Cyfryzacji, b.d.) zobowiązuje operatorów usług kluczowych do

przeprowadzania audytów bezpieczeństwa systemów teleinformatycznych raz na dwa lata. Do realizacji audytu bezpieczeństwa zobowiązane są również podmioty publiczne i prywatne, które korzystają z dofinansowania, np. z programu NFZ czy z programu Cyberbezpieczny Samorząd. Audyty te mają za zadanie potwierdzenie czy otrzymane środki z dotacji zostały właściwie wykorzystane do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych. Każdy podmiot zarówno publiczny i prywatny powinien cyklicznie przeprowadzić audyt bezpieczeństwa informacji, często zwany również jako audyt cyberbezpieczeństwa.

Audytowanie charakteryzowane jest zgodnie z szeregiem zasad, dzięki którym proces ten staje się skutecznym i wiarygodnym narzędziem wspierającym polityki i środki nadzoru kierownictwa, dostarczając informacji na podstawie których organizacja może doskonalić swoje efekty działania. Aby zapewnić, że wnioski wynikające z przeprowadzonego audytu są właściwe i wystarczające audytorzy muszą przestrzegać pewnych warunków i zasad. Audytowanie powinno opierać się na siedmiu uniwersalnych zasadach. Rzetelność definiowana jako podstawa profesjonalizmu, która powinna gwarantować uczciwe, etyczne i nacechowane odpowiedzialnością podejście do czynności audytorskich. Obowiązek uczciwego przedstawiania wyników, czyli wymóg postępowania i obrazowania spraw zgodnie z prawdą. Należyta staranność, czyli pracowitość i rozsądek w audytowaniu. Poufność, czyli konieczność zapewnienia bezpieczeństwa informacji na każdym etapie procesu audytu. Niezależność audytora rozumiana jako podstawa bezstronności audytu oraz obiektywności wyciągniętych przez audytora wniosków. Podejście oparte na dowodach, które polega na racjonalnym, ich pozyskiwaniu a następnie analizie danych i obiektywnej ocenie w celu uzyskiwania wiarygodnych wniosków. Podejście oparte na ryzyku odnoszące się do konieczności uwzględniania ryzyk i szans związanych z planowaniem i realizacją audytu (Global Cert, 2025).

Tabela 3. Podstawowe zasady audytowania – 7 uniwersalnych zasad audytowania

Zasada 1	Rzetelność: podstawa profesjonalizmu	<ul style="list-style-type: none"> wykonywanie swojej pracy uczciwie, sumiennie i odpowiedzialnie stosowanie się do wszystkich mających zastosowanie „wymagań prawa”, „zgodnie z prawdą”. wykazywanie się kompetencją podczas wykonywania swojej pracy wykonywanie swojej pracy w sposób bezstronny tj. uczciwość i bez uprzedzeń wyczerpujący na wszelkie wpływy, które mogą oddziaływać na dokonywane oceny podczas przeprowadzania audytu
Zasada 2	Uczciwe przedstawianie wyników: obowiązek przedstawiania spraw dokładnie i zgodnie z prawdą	<ul style="list-style-type: none"> ustalenia z audytu, wnioski z audytu oraz raporty z audytu powinny odzwierciedlać działania audytowe dokładnie i zgodnie z prawdą <p>Obiektywność w prezentacji wyników audytu jest kluczowa, ponieważ tylko wtedy organizacje mogą podejmować świadome decyzje dotyczące swoich systemów zarządzania. Rzetelne i oparte na dowodach przedstawienie wyników pozwala na pełne zrozumienie sytuacji i podjęcie działań naprawczych tam, gdzie to konieczne. Bezstronność to podstawa.</p> <ul style="list-style-type: none"> ustalenia z audytu, wnioski z audytu oraz raporty z audytu powinny odzwierciedlać działania audytowe dokładnie i zgodnie z prawdą odnotowywanie w raporcie znaczących przeszkód napotkanych podczas audytu obowiązek przedstawiania spraw dokładnie i zgodnie z prawdą nierozstrzygniętych lub rozbieżnych opinii pomiędzy zespołem audytującym a audytowanym komunikacja zgodna z prawdą, dokładna, obiektywna, na czas, zrozumiała i pełna staranność odpowiednia do ważności zadań zdolność do racjonalnego osądzania we wszystkich sytuacjach audytowych
Zasada 3	Należyta staranność zawodowa: pracowitość i rozsądek w audytowaniu	<ul style="list-style-type: none"> dyskrecja w użyciu i ochronie informacji, do których mają dostęp w wyniku wykonywania swoich obowiązków informacje audytowe nie mogą być wykorzystywane dla osobistych korzyści audytora, klienta audytu czy też w sposób szkodliwy dla uzasadnionych interesów audytowanego poprawne obchodzenie się z wrażliwymi i poufnymi informacjami
Zasada 4	Poufność: bezpieczeństwo informacji	

Zasada 5	<p>Niezależność:</p> <p>podstawa do bezstronności audytów i obiektywności wniosków audytowych</p>	<p>Niezależność audytorów to kolejna zasada, która ma ogromne znaczenie w procesie audytowania. Audytorzy muszą być bezstronni i niezależni od obszarów, które audytują, aby móc formułować obiektywne wnioski. Niezależność zapewnia, że audyty są przeprowadzane bez zewnętrznych wpływów, co jest niezbędne dla zachowania integralności całego procesu. Dzięki temu organizacje mogą być pewne, że wyniki audytu są wolne od uprzedzeń czy nacisków, co gwarantuje uczciwość całego procesu.</p> <ul style="list-style-type: none"> niezależni od działań podlegających audytowi, o ile jest to wykonalne we wszystkich przypadkach powinni działać w sposób wolny od uprzedzeń i konfliktu interesów w przypadku audytów wewnętrznych powinni być niezależni od audytowanej funkcji, jeżeli jest to wykonalne powinni zachować obiektywność podczas całego procesu audytu, aby ustalenia i wnioski audytu były oparte wyłącznie na dowodach audytowych
Zasada 6	<p>Podjęcie oparte na faktach:</p> <p>racjonalna metoda uzyskiwania wiarygodnych i powtarzalnych wniosków audytowych</p>	<p>Jedną z kluczowych zasad jest dowód z audytu. Bardzo ważne jest uzyskiwanie wiarygodnych i powtarzalnych dowodów, które stanowią podstawę do formułowania wniosków z audytu. Dowody te muszą być zbierane systematycznie i zgodnie z ustalonymi procedurami, co zapewnia, że wyniki audytu są solidne i mogą być wykorzystane do doskonalenia systemów zarządzania. Tylko na podstawie rzetelnych dowodów organizacje mogą podejmować działania, które rzeczywiście przyczynią się do poprawy ich funkcjonowania. Bez dowodów, audyt traci sens.</p> <ul style="list-style-type: none"> dowody audytowe powinny być weryfikowalne i oparte na próbkach dostępnych informacji (określony czas i ograniczone zasoby) należy zastosować odpowiednie pobieranie próbek, ponieważ jest to ściśle związane z pewnością, którą można zawrzeć we wnioskach z audytu
Zasada 7	<p>Podjęcie oparte na ryzyku:</p> <p>podjęcie audytu uwzględniające ryzyka i szanse związane z audytem</p>	<ul style="list-style-type: none"> istotny wpływ na planowanie, przeprowadzanie i raportowanie audytów audyty koncentrują się na sprawach istotnych dla klienta audytu oraz na osiągnięciu celów programu audytów

Źródło: Global Cert (2025). Norma ISO 19011 – Wytyczne dotyczące audytowania systemów zarządzania. Pobrano z: <https://certyfikacja-iso.pl/2025/01/17/norma-iso-19011-wytyczne-dotyczace-audytowania-systemow-zarzadzania/> (dostęp: 20.09.2025).

Przestrzeganie powyższych zasad jest kluczowe dla wiarygodności i skuteczności procesu audytowania, buduje zaufanie między audytorem a audytowanym oraz pozwala na podejmowanie trafnych decyzji. Audyty w organizacji przeprowadza się zgodnie z programem audytów. Program audytów stanowi jeden lub wiele audytów zaplanowanych w określonych ramach czasowych i mających określony cel.

Proces audytowania – działania audytorskie

Audyt to proces wieloetapowy, który wymaga odpowiedniego przygotowania, starannego badania oraz szczegółowej analizy wyników. Każdy z tych etapów odgrywa kluczową rolę w identyfikacji obszarów wymagających działań korygujących oraz poprawie efektywności procesów w organizacji. Dzięki jasno określonemu przebiegowi audytu możliwe jest zapewnienie zgodności działań z przepisami wewnętrznymi organizacji i obowiązującymi standardami. Proces audytowania to usystematyzowane, niezależne badanie mające na celu ocenę zgodności działań i efektywności procesów w organizacji. Składa się z planowania, zbierania danych, analizy ryzyka, raportowania oraz działań następczych (korygujących). Kluczowe działania obejmują wywiady, przegląd dokumentacji, obserwację i audytowanie na miejscu. Prowadzenie audytu to proces niezależnej oceny systemu, procesu, produktu lub organizacji pod kątem zgodności z określonymi kryteriami, takimi jak standardy, przepisy prawa lub procedury wewnętrzne. Audytorzy zbierają dane poprzez wywiady, analizę dokumentów i obserwację, a następnie identyfikują obszary do poprawy i wydają zalecenia. Kluczowe zasady prowadzenia audytu to niezależność, obiektywizm i metodyczne zbieranie dowodów, a cały proces kończy się przygotowaniem raportu zawierającego wnioski i działania naprawcze. Przygotowanie do audytu to kluczowy etap, który obejmuje określenie przedmiotu audytu oraz zakresu badania. Podczas właściwego procesu audytu audytorzy zbierają dane poprzez wywiady z pracownikami, analizę dokumentacji oraz obserwację działań w praktyce. Badanie obejmuje kontrolę zgodności procesów z obowiązującymi procedurami i standardami oraz identyfikację wszelkich niezgodności lub obszarów wymagających poprawy. Audytorzy analizują dokumentację, takie jak przepisy wewnętrzne organizacji, procedury oraz wyniki wcześniejszych audytów. Celem przygotowania jest również identyfikacja potencjalnych

obszarów ryzyka i opracowanie planu działań, który pozwoli przeprowadzić audyt zgodnie z określonymi standardami i procedurami (Hotiuk, 2024). Planowanie audytu ma za cel odpowiednie przeprowadzenie działań audytorskich na miejscu. Plan audytu powinien obejmować:

- cele i zakres audytu,
- kryteria audytu i wszystkie dokumenty,
- daty i miejsca, gdzie czynności audytorskie mają być prowadzone,
- rozpoznanie organizacyjnych i funkcjonalnych jednostek oraz procesów,
- oczekiwany czas i trwanie czynności audytorskich na miejscu.
- Planując audyt należy wziąć pod uwagę następujące kwestie:
 - skład zespołu audytowego i jego ogólne kompetencje,
 - odpowiednie techniki pobierania próbek,
 - możliwości poprawy skuteczności i wydajności działań audytowych,
 - ryzyko związane z osiągnięciem celów audytowych wynikających z nieefektywnego zaplanowania audytu,
 - ryzyko dla audytowanego będące wynikiem przeprowadzenia audytu i działań audytorów na jego terenie.

Planowanie audytu ma za cel odpowiednie przeprowadzenie działań audytorskich na miejscu. Plan audytu może obejmować:

- ustalenie kluczowego przedstawiciela audytowanego biorącego udział w audycie,
- język roboczy i sprawozdawczy audytu,
- określenie ról i obowiązków członków zespołu audytorskiego i innych towarzyszących osób,
- tematy raportów audytorskich, format i struktura, oczekiwana data wydania,
- ustalenia logistyczne (podróż, udogodnienia na miejscu, itd.).

Planowanie audytu ma za cel odpowiednie przeprowadzenie działań audytorskich na miejscu. Do planowania audytu powinno się przyjąć podejście oparte na ryzyku, w szczególności ryzyku nieosiągnięcia celów audytu. Planowanie audytu powinno brać pod uwagę ryzyko związane z działaniami audytowanymi w procesach audytowanego i stanowić podstawę porozumienia pomiędzy klientem audytu, audytowanym i zespołem audytowanym

w zakresie przeprowadzenia audytu. Należy mieć na uwadze, iż, skala i zawartość audytu mogą się różnić, na przykład między audytami początkowymi i kolejnymi, a także między audytami wewnętrznymi i zewnętrznymi. Planowanie audytu powinno być wystarczająco elastyczne, aby umożliwić zmiany, które mogą stać się konieczne w miarę postępu działań audytowych. Plan audytu powinien być przedstawiony audytowanemu (klientowi audytu) do zapoznania się i akceptacji.

Cele audytu: audyt polega na zbadaniu aktualnego stanu zabezpieczenia zasobów informacyjnych pod względem: poufności, integralności i dostępności, wskazaniu niezgodności oraz przygotowaniu rekomendacji związanych z wprowadzeniem mechanizmów służących do uzyskania bezpieczeństwa informacji, zgodnego z normą. W praktyce audyt bezpieczeństwa informacji w oparciu o normę ISO/IEC 27001 ma na celu określenie zgodności istniejącego systemu zarządzania bezpieczeństwem informacji (SZBI) z wymaganiami zawartymi w normie.

Kryteria audytu: audyt zawsze musi odnosić się do założonych kryteriów. Kryteria audytu są to wymagania jakie organizacja ma do spełnienia w zakresie bezpieczeństwa informacji. Kryteria audytu obejmują następujące wymagania:

- zobowiązania wynikające z zawartych umów,
- wymagania zawarte w przepisach prawa,
- dokumentacja systemowa,
- normy (ISO/IEC 27001).

Działania audytowe: audyt bezpieczeństwa informacji łączy kompleksowy przegląd procedur postępowania w przypadku ataku cybernetycznego w organizacji oraz ocenę polityki bezpieczeństwa, mającej na celu codzienną prewencję przed wyciekami danych oraz innymi skutkami cyberataków, a także przestrzeganiem bezpiecznych praktyk w ochronie systemów i danych. Właściwie przeprowadzony audyt powinien być zaplanowany i przeprowadzony w sposób bardzo przemyślany. Program audytu powinien zostać zaplanowany i uwzględniać wyniki poprzednich audytów. Częstotliwość i metody przeprowadzania audytu, przyjęte kryteria i zakres, którego on dotyczy, powinny być z góry ustalone. Wybór audytorów i sposób przeprowadzenia audytu powinny zapewnić obiektywność i bezstronność procesu. Audytorzy nie powinni prowadzić audytów dotyczących ich własnej pracy. Wymagania i odpowiedzialność za planowanie i przeprowadzanie

audytów w organizacji oraz za raportowanie ich wyników i utrzymywanie zapisów powinny zostać określone w udokumentowanej procedurze. Audytorzy powinni posiadać udokumentowane uprawnienia potwierdzające wiedzę, doświadczenie oraz umiejętności.

Proces audytu bezpieczeństwa informacji obejmuje kilka kluczowych etapów (Wójcik, 2017):

ETAP 1. Inicjowanie audytu – wyznaczenie zespołu audytującego.

W celu wyznaczenia zespołu audytowego potrzebne są określone działania, w tym:

1. Wyznaczenie audytorów oraz audytora wiodącego (kierownika zespołu) do danego audytu oraz sprawdzenie uprawnień, kompetencji i doświadczenia audytorów.
2. Określenie celów audytu, jego zakresu i kryteriów. Audyt ma sprawdzić zgodność stanu zastanego z wymaganym. Zgodność ta jest oceniana na podstawie przyjętych kryteriów oceny.
3. Określenie wykonalności audytu. Zaleca się określenie wykonalności audytu z uwzględnieniem takich czynników jak:
 - dostępność wystarczających i odpowiednich informacji,
 - możliwość potrzebnej współpracy z audytowanym,
 - adekwatny czas i zasoby (w tym dostępność osób i dostęp do obszarów audytowanych).
4. Nawiązanie pierwszego kontaktu z audytowanym. Pierwszy kontakt z audytowanym może być nieformalny lub formalny, ale zaleca się, żeby był nawiązany przez audytorów odpowiedzialnych za zarządzanie programem lub przez audytora wiodącego. Celem pierwszego kontaktu jest:
 - ustalenie sposobów komunikacji z przedstawicielem audytowanego,
 - potwierdzenie uprawnień do przeprowadzenia audytu,
 - dostarczenie informacji dotyczących proponowanego harmonogramu oraz składu zespołu audytującego,
 - wnioskowanie o dostęp do stosownych dokumentów,
 - określenie zasad bezpieczeństwa mających zastosowanie w danym miejscu,
 - dokonanie ustaleń dotyczących audytu,

- uzgodnienie uczestnictwa obserwatorów oraz przewodników dla zespołu audytującego.

ETAP 2. Przegląd dokumentacji.

Przed podjęciem działań audytowych zaleca się dokonanie przeglądu dokumentacji w celu określenia zgodności kryteriów audytu z normami, np. technicznymi lub dotyczącymi zarządzania bezpieczeństwem informacji. Dokumentacja ta może obejmować odpowiednie dokumenty i zapisy dotyczące systemu zarządzania, a także raporty z poprzednich audytów. Podczas przeglądu zaleca się wzięcie pod uwagę wielkości, charakteru i złożoności przedsiębiorstwa oraz celów i zakresu audytu. Jeżeli dokumentacja okaże się nieodpowiednia, audytor wiodący powinien poinformować o tym odbiorcę audytu, osoby odpowiedzialne za zarządzanie programem audytów oraz audytowanego. Zaleca się podjęcie decyzji o kontynuacji audytu albo jego zawieszeniu do czasu rozwiązania kwestii związanych z dokumentacją.

ETAP 3. Planowanie działań audytowych realizowanych na miejscu.

Audytor powinien przygotować plan przeprowadzenia audytu stanowiący podstawę do uzgodnień pomiędzy odbiorcą audytu, zespołem audytującym oraz audytowanym. Zaleca się, żeby plan ułatwiał ustalenie terminów i koordynację działań audytowych. Plan audytu powinien być przejrzany i zaakceptowany przez odbiorcę audytu oraz przedstawiony audytowanemu przed rozpoczęciem działań audytowych. Wszelkie zastrzeżenia audytowanego powinny być rozstrzygnięte wspólnie – przez audytora, audytowanego i odbiorcę audytu. Zaleca się, żeby przed kontynuowaniem audytu każda zmiana planu została uzgodniona pomiędzy stronami, których ona dotyczy.

ETAP 4. Przeprowadzanie działań audytowych.

Audyt powinien rozpocząć się od spotkania otwierającego, na którym powinien być obecny audytor oraz osoby odpowiedzialne za audytowane dziedziny, np. kierownicy działów. Spotkanie otwierające powinno się odbyć, aby potwierdzić plan audytu, wyjaśnić jakie czynności będą przeprowadzone i ustalić sposób porozumiewania. Spotkanie otwierające powinno się odbyć z osobami odpowiedzialnymi za audytowane funkcje i procesy. Celem spotkania otwierającego jest:

- potwierdzenie planu audytu,
- krótkie zaprezentowanie, jak będą wykonywane działania audytowe,
- potwierdzenie metod komunikowania się,

- umożliwienie audytowanemu zadawania pytań.

Podczas audytu audytor wiodący powinien zgłaszać wszelkie zastrzeżenia i okresowo informować audytowanego i odbiorcę audytu o postępach w procesie audytu. Jest to dobra praktyka. Dowody zebrane podczas audytu, które wskazują na bezpośrednie i znaczące uchybienia, audytor powinien bezzwłocznie przekazać audytowanemu i jeżeli to właściwe, odbiorcy audytu. Każda sprawa dotycząca problemu wybiegającego poza zakres audytu powinna być odnotowana i przedstawiona audytorowi wiodącemu w celu ewentualnego zakomunikowania odbiorcy audytu i audytowanemu. Jeżeli dostępne dowody wskazują na to, że cele audytu są niemożliwe do osiągnięcia, zaleca się, żeby audytor wiodący przedstawił odbiorcy audytu i audytowanemu przyczyny w celu podjęcia określonych działań. Działania te mogą obejmować potwierdzenie audytu lub zmianę jego planu, celów lub zakresu lub jego zakończenie. Każda potrzeba zmiany zakresu, która może pojawić się na skutek realizacji działań audytowych, powinna być omówiona z odbiorcą, przez niego zatwierdzona oraz jeżeli to właściwe, sprawdzona i zatwierdzona przez audytowanego.

Zbieranie i weryfikowanie informacji - informacje dotyczące celów, zakresu oraz kryteriów audytu, łącznie z informacją dotyczącą oddziaływania pomiędzy funkcjami, działaniami i procesami, powinny być gromadzone poprzez odpowiednie pobieranie próbek podczas audytu i weryfikowane. Tylko uzyskana podczas audytu informacja, która jest możliwa do zweryfikowania, może stanowić dowód. Taka informacja powinna być zapisana. Gromadzenie dowodów to zbieranie informacji, które są istotne dla celów, zakresu i kryteriów audytu, w tym informacji odnoszących się do wzajemnego oddziaływania pomiędzy funkcjami, czynnościami i procesami. Zebrane informacje mogą zostać uznane za dowody audytowe, gdy są zweryfikowane przez audytorów i zaprotokołowane (zapisane). Najczęściej spotykane metody zbierania informacji (źródła informacji/dowodów) to:

- rozmowy,
- wywiady,
- obserwacje działań i procesów,
- przegląd dokumentów,
- przegląd zapisów, rejestrów,
- protokoły,

- streszczenia danych, analizy, wskaźniki,
- raporty,
- bazy danych skomputeryzowanych i witryny sieci www.

Dowody audytowe prowadzące do ustaleń audytowych powinny być rejestrowane. Jeśli zespół audytowy podczas zbierania obiektywnych dowodów dowie się o nowych bądź zmienionych okolicznościach albo zagrożeniach lub szansach, zespół powinien odpowiednio się nimi zająć. Udokumentowane informacje przygotowane do audytu oraz wynikające z niego, powinny być przechowywane przynajmniej do zakończenia audytów lub zgodnie z programem audytowym. Udokumentowane informacje stworzone podczas procesu audytowania z udziałem poufnych lub zastrzeżonych informacji powinny być przez cały czas odpowiednio chronione przez członków zespołu audytowego. Członkowie zespołu audytowego powinni gromadzić i przeglądać informacje istotne dla ich zadań związanych z audytem oraz przygotowywać udokumentowane informacje na temat audytów, wykorzystując wszelkie odpowiednie media.

Gromadzenie dowodów:

1. Wybór źródła informacji.
2. Zbieranie informacji za pomocą odpowiednich próbek.
3. Formułowanie dowodów audytowych.
4. Ocena dowodów zgodnie z kryterium audytu.
5. Zebranie i przygotowanie wyników audytu.
6. Przekazanie zaleceń audytowanego.

Gromadząc dowody należy pamiętać:

- że w razie wątpliwości co do oceny danego dowodu zawsze możesz zwrócić się do audytora wiodącego i/lub poprosić audytowanego o przedstawienie innego dowodu na potwierdzenie wcześniejszej oceny,
- aby skupić się na kryteriach audytu. Informacje, które nie dotyczą audytowanego zakresu nie powinny być poruszane i nie powinny być rejestrowane. Nie powinny one także wpływać na ocenę dowodów odnoszących się do danego audytu,
- że audytowany może być zdenerwowany i/lub zestresowany. Dlatego staraj się podczas interakcji minimalizować napiętą atmosferę, np. nie pośpieszając rozmówcy,

- kulturze osobistej oraz zasadach *savoir-vivre*: nie należy przerywać audytowanemu, nie należy wprowadzać zbyt luźnej atmosfery, należy unikać tematów drażliwych i osobistych,
- aby zapisywać je krótko i zwięźle; notatki mogą być częścią raportu z audytu i służyć audytorom w kolejnych audytach,
- że najlepszym sposobem dokumentowania dowodu jest powołanie się na konkretny zapis – nazwa dokumentu, wpis w rejestrze czy bazie danych, informacja udostępniona na stronie www lub w mediach społecznościowych. Jeżeli jest to konieczne, można się posiłkować zrzutami ekranu, jednak nie należy nadużywać tej metody.

Opracowanie ustaleń z audytu (ustalenia na podstawie audytu) – Ustalenia mogą wskazywać na zgodność lub niezgodność z kryteriami, np. normami technicznymi. Jeżeli jej wykazanie było jednym z celów audytu, ustalenia mogą wskazać sposób poprawy.

Wnioski z audytu – Zespół audytujący (audytor) powinien naradzić się przed spotkaniem zamykającym audyt w celu:

- sprawdzenia, co ustalono podczas audytu i jakie informacje zebrano w związku z obranymi celami,
- uzgodnienia wniosków z uwzględnieniem niepewności związanej z audytowaniem,
- przygotowania rekomendacji, jeżeli taki jest jeden z wyznaczonych celów,
- przedyskutowania działań po audycie, jeżeli uwzględniono je w planie.

Spotkanie zamykające – przeprowadzenie spotkania zamykającego. Spotkanie zamykające powinno się odbyć, aby zaprezentować wyniki audytu w taki sposób, by mieć pewność, że są one zrozumiałe i uznane przez audytowanego, a także uzgodnić czas niezbędny do zaprezentowania wszelkich planów działań naprawczych przez audytowanego. Spotkanie zamykające prowadzone przez audytora powinno odbyć się w celu przedstawienia ustaleń oraz wniosków w taki sposób, aby były one zrozumiałe i potwierdzone przez audytowanego. Zaleca się ustalenie terminu przedstawienia planu działań korygujących i zapobiegawczych przez audytowanego. W spotkaniu zamykającym powinni uczestniczyć wszyscy audytowani, ale może w nim uczestniczyć także odbiorca audytu i inne strony. Jeżeli to konieczne,

zaleca się, żeby audytor poinformował audytowanego o sytuacjach zaistniałych w trakcie audytu, które mogą negatywnie wpłynąć na ocenę wniosków z audytu. W niektórych przypadkach, np. po audycie w małym przedsiębiorstwie, spotkanie zamykające może polegać tylko na zakomunikowaniu ustaleń i wniosków. Zazwyczaj jednak powinno mieć charakter formalny i być zgodne ze wszystkimi zasadami, łącznie ze składaniem podpisów na liście obecności. Wszelkie rozbieżne opinie zespołu audytującego i audytowanego dotyczące ustaleń i wniosków powinny być przedyskutowane i, jeśli to możliwe, uzgodnione. W przypadku braku zgodności opinii zaleca się zapisanie obu opinii w raporcie z audytu. Raport powinien zawierać rekomendacje dotyczące sposobu poprawy stanu, jeżeli taki jest jeden z celów audytu. W spotkaniu otwierającym i zamykającym powinien uczestniczyć także przedstawiciel najwyższego kierownictwa audytowanego, może także brać udział przedstawiciel klienta audytu. Spotkania otwierające i zamykające mają ustaloną w normie PN-EN ISO 19011:2018 strukturę i zakres. Ze spotkania otwierającego i zamykającego należy przygotować listę obecności, gdzie podpiszą się wszyscy uczestniczący – zarówno po stronie zespołu audytującego, jak i audytowanego i klienta audytu

ETAP 5. Zakończenie audytu.

Audyty będzie zakończony, gdy zostaną wykonane wszystkie działania opisane w planie i zostanie rozesłany zatwierdzony raport. Dokumenty dotyczące audytu powinny być zachowane lub zniszczone na podstawie uzgodnień pomiędzy stronami uczestniczącymi oraz zgodnie z procedurami, mającymi zastosowanie przepisami oraz wymaganiami wynikającymi z umów. Zespół audytujący oraz osoby odpowiedzialne za zarządzanie programem audytów nie powinny ujawniać osobom trzecim zawartości dokumentów, innych informacji uzyskanych podczas audytu lub raportu z audytu bez jasno wyrażonego pozwolenia odbiorcy audytu i jeżeli to właściwe, audytowanego, chyba że działanie takie jest nakazane przez prawo. Jeżeli wymagane jest ujawnienie zawartości dokumentu dotyczącego audytu, zaleca się jak najszybsze poinformowanie o tym odbiorcy audytu i audytowanego.

Przygotowanie, zatwierdzenie i rozpowszechnianie raportu dotyczącego audytu – po zakończeniu badania audytorzy dokonują analizy wyników, identyfikując nieprawidłowości i obszary wymagające działań korygujących. Kluczowym elementem tego etapu jest przygotowanie raportu z audytu, który zawiera szczegółowe rekomendacje dotyczące poprawy

procesów i wdrażania działań naprawczych. Raport ten jest podstawą do podejmowania decyzji przez zarząd organizacji i wyznaczenia priorytetów w zakresie działań korygujących. Każdy audyt kończy się raportem, w którym oprócz wskazania luk i braków zamieszcza się również propozycję działań naprawczo-korygujących. W praktyce raport podzielony jest na dwie części – pierwsza część zawiera sumaryczne zestawienie wyników audytu w odniesieniu do wymagań bezpieczeństwa informacji, a druga – wytyczne do doskonalenia i zakres prac, które zwiększą poziom bezpieczeństwa informacji. Niezwykle ważne jest, aby sam audyt, jak i rekomendacje, dostosowane były do branży i specyfikacji organizacji, a także do już funkcjonujących procedur (Borkowski, b.d.). Raport z audytu bezpieczeństwa informacji to dokument, który daje odpowiedź na pytanie, czy organizacja spełnia normy i standardy dotyczące bezpieczeństwa informacji.

Przygotowanie raportu dotyczącego audytu – audytor jest odpowiedzialny za przygotowanie i treść raportu dotyczącego audytu. Raport z audytu powinien dostarczyć pełny, dokładny, zwięzły i jasny protokół z audytu i powinien zawierać konkluzje z audytu. Zaleca się, żeby raport ten zawierał kompletne, dokładne, zwięzłe i jasne informacje dotyczące audytu. Powinien obejmować:

- wskazanie celów audytu,
- podanie czasu trwania audytu,
- określenie zakresu audytu, w szczególności wskazanie audytowanych jednostek organizacyjnych i funkcjonalnych lub audytowanych procesów,
- wskazanie odbiorcy audytu (identyfikacja audytowanego – klienta audytu),
- wskazanie audytora wiodącego i członków zespołu audytującego (identyfikacja zespołu audytorów i uczestników ze strony audytowanego),
- podanie daty i miejsca prowadzenia działań audytowych na miejscu.
- Raport powinien powoływać się na:
 - kryteria dotyczące audytu,
 - ustalenia wynikające z audytu tj. ustalenia audytowe i związane z nimi dowody,
 - wnioski wpływające z audytu,
 - oświadczenie o stopniu spełnienia kryteriów audytu,

- wszelkie nierozstrzygnięte rozbieżne opinie między zespołem audytowym a audytowanym.

Raport dotyczący audytu jest tworzony na podstawie indywidualnego wzoru dostosowanego do potrzeb odbiorcy audytu. Najistotniejszym elementem każdego raportu powinny być wnioski z audytu – jeśli zostało to określone w planie audytu, wnioski z audytu mogą prowadzić do zaleceń dotyczących ulepszeń lub przyszłych działań związanych z audytem. Wyniki audytu mogą wskazywać na zgodność lub niezgodność z kryteriami audytu bądź wskazywać na możliwości ulepszenia. Wyniki audytu, niezależnie od rezultatu, powinny być zaprotokołowane i wsparte dowodami audytowymi. Dowody audytowe powinny być oceniane na podstawie kryteriów audytowych w celu ustalenia wyników audytu. Należy podjąć każdą próbę rozwiązania wszelkich rozbieżnych opinii dotyczących dowodów lub ich oceny przed ustaleniem ostatecznych wyników audytu. Ustalenia wyników audytu mogą wskazywać na zgodność lub niezgodność z kryteriami audytowymi. Wyniki audytu wskazujące na niezgodność powinny być omówione z audytowanym, aby wyeliminować możliwe różnice w interpretacji dowodów i wyników audytu. Dla każdej niezgodności powinien zostać przygotowany protokół niezgodności. Protokół niezgodności powinien zawierać co najmniej zdefiniowanie niezgodności, wskazanie, którego wymagania normy / zabezpieczenia dotyczy oraz jakie dowody wskazują na istnienie niezgodności. Ważne jest, aby określić miejsce wystąpienia niezgodności. Protokół niezgodności powinien być podpisany przez audytora i przedstawiciela audytowanej jednostki organizacyjnej, aby potwierdzić zidentyfikowanie niezgodności podczas konkretnej sesji audytowej. Przygotowując raport z audytu trzeba pamiętać, że raport z audytu będzie dokumentem poddawany ocenie podczas kolejnych audytów i powinien być przygotowany rzetelnie.

Zatwierdzenie i rozpowszechnianie raportu dotyczącego audytu – raport dotyczący audytu powinien być przekazany w uzgodnionym terminie. Jeżeli nie jest to możliwe, należy zakomunikować przyczyny opóźnienia odbiorcy audytu oraz uzgodnić nowy termin przesłania raportu. W przypadku opóźnienia, powody powinny zostać przekazane audytowanemu i klientowi audytu. Raport z audytu powinien być opatrzony datą, zweryfikowany i zaakceptowany przez wszystkie strony audytu. Raport powinien być zatwierdzony, a następnie rozesłany do odbiorców wskazanych przez

odbiorcę audytu. Raport dotyczący audytu jest własnością odbiorcy audytu. Członkowie zespołu audytującego (audytor) oraz wszyscy odbiorcy raportu powinni przestrzegać zasad dotyczących poufności raportu. Przygotowując raport z audytu należy pamiętać, że zawarte w nim wnioski i wyniki powinny opierać się na zgromadzonych wcześniej dowodach. Jeżeli w jakimś zakresie nie udało się zebrać dowodów, które odnosiłyby się do poszczególnych kryteriów, należy to odnotować, nie oceniając spełnienia lub niespełnienia danego kryterium. W raporcie muszą znaleźć się wszelkie parametry audytu, które zostały ustalone na etapie inicjacji audytu, w szczególności daty przeprowadzenia audytu, czas audytu na miejscu, skład zespołu audytowego, cele, zakres i kryteria audytu. Pamiętaj także, żeby raport miał datę jego sporządzenia i podpis audytora wiodącego.

ETAP 6. Przeprowadzenie działań poaudytowych (działania po audycie).

Wnioski wypływające z audytu mogą wskazywać na potrzebę podjęcia działań korygujących, naprawczych lub doskonalących, jeżeli ma to zastosowanie. Takie działania są zwykle określane i podejmowane przez audytowanego w uzgodnionym terminie oraz nie są uważane za część audytu. Zaleca się, żeby audytowany informował odbiorcę audytu o statusie tych działań. Niezgodność to brak spełnienia jednego z kryteriów audytu. Niezgodności mogą być stopniowane w zależności od kontekstu organizacji i jej ryzyka (skala ilościowa lub jakościowa). Niezgodności powinny zostać wyeliminowane w czasie uzgodnionym z audytowanym i powinno zostać zweryfikowane wdrożenie i skuteczność tych działań. Niezgodności i towarzyszące im dowody z audytów powinny być rejestrowane. Potencjalne niezgodności, które pojawią się w trakcie gromadzenia dowodów, powinny być przedyskutowane wśród członków zespołu audytowego już czasie audytu. Niezgodności powinny zostać sprawdzone przez audytowanego w celu uzyskania potwierdzenia, że dowody audytowe są dokładne i że niezgodności są zrozumiałe dla audytowanego. Niezgodności wraz z terminem ich korekty powinny zostać ujęte w raporcie z audytu. Z niezgodnościami związane są działania korekcyjne oraz działania korygujące. Działaniami korekcyjnymi można określić wszystkie działania, które są podejmowane w celu usunięcia wykrytej niezgodności. Działaniami korygującymi można określić działania podjęte w celu wyeliminowania przyczyny wykrytej niezgodności. Działania korekcyjne i korygujące powinny mieć ustalony z audytowanym termin ich wdrożenia i oceny ich skuteczności. Audytujący powinien informować

osoby zarządzające audytem i zespołem audytowym o statusie działań korekcyjnych i korygujących. Wynik oceny działań korekcyjnych i korygujących musi trafić do klienta audytu, zazwyczaj jako dodatkowy raport. Klient audytu powinien dostać potwierdzenie, że działania eliminujące niezgodność były skuteczne. Działania poaudytowe:

- rejestracja niezgodności w odpowiednim rejestrze w organizacji,
- przygotowanie planu zarządzania niezgodnością,
- analiza ryzyka związanego z niezgodnością,
- wdrożenie działań korekcyjnych,
- wdrożenie działań korygujących,
- ocena skuteczności wdrożenia działań korygujących.

Zarządzając niezgodnościami trzeba mieć na uwadze, żeby dostarczony przez audytowanego plan zarządzania niezgodnościami zawierał takie pozycje, jak analiza przyczyn wystąpienia niezgodności, terminy wdrożenia działań i osoby odpowiedzialne za ich wdrożenie, a także ocena skuteczności wdrożonych działań.

ETAP 7. Weryfikacja zakończenia i skuteczności działań korygujących.

Weryfikacja ta może być częścią następnego audytu, którego celem będzie także sprawdzenie skuteczności i efektywności działań korygujących. Program audytu może określać udział zespołu audytującego w działaniach po audycie, które przynoszą dodatkową korzyść dzięki już zdobytemu przez ten zespół doświadczeniu. Należy zadbać o bezstronność zespołu, jeżeli będzie on wykonywał dodatkowe działania audytowe.

Proces przeprowadzania audytu to nie tylko kontrola, ale także element wspierający poprawę efektywności organizacji. Regularne przeprowadzanie audytów pozwala na identyfikację potencjalnych ryzyk oraz wdrażanie skutecznych rozwiązań. Dzięki cyklicznym audytom bezpieczeństwa mamy pewność, że wszelkie ewentualne nieprawidłowości zostaną zidentyfikowane zanim pojawi się potencjalne zagrożenie. Pozwoli to organizacji na zminimalizowanie ryzyka utraty danych i utraty ciągłości działania organizacji. Najlepsze rezultaty przynosi audyt przeprowadzony przez niezależnych bezstronnych audytorów (Jurkiewicz, 2023).

Podsumowanie

Przeprowadzenie audytu bezpieczeństwa ma istotne znaczenie dla zapewnienia odpowiedniego poziomu ochrony dla organizacji lub instytucji. Pozwala on na identyfikację luk w zabezpieczeniach, wzmocnienie procedur oraz ochronę danych i infrastruktury przed różnymi zagrożeniami. Audyt ma dostarczać obiektywnych dowodów, że procesy działają zgodnie z wymaganiami norm i przepisów, a nie skupiać się na wychwyceniu każdej nieprawidłowości za wszelką cenę. Może być pomocny w osiągnięciu celów organizacyjnych, bowiem stanowi systematyczne i metodyczne podejście do oceny skuteczności zarządzania organizacją. Należy podkreślić, że audyt stanowi skuteczny i niezawodny instrument wspierający politykę bezpieczeństwa obiektu i umożliwiający skontrolowanie zarządzania bezpieczeństwem. Dostarcza informacji, które są niezbędne, by zadbać o bezpieczeństwo w organizacji. W przeprowadzaniu audytu ważne są (Wójcik, 2019): uczciwość, rzetelność, profesjonalizm w działaniu, poufność, niezależność, ustalenie faktów, uwzględnienie trudności i określenie prawdopodobieństwa, że cele audytu zostaną osiągnięte (ta zasada jest narzucona przez normę ISO 19011). Należy przestrzegać powyższych zasad, aby wyniki audytu były jednoznaczne i aby można było spodziewać się, że inni audytorzy uzyskają podobne wyniki w podobnych okolicznościach. Można go zatem potraktować jako narzędzie do doskonalenia organizacji i przyniesienia jej wartości dodanej (Qualitywise, b.d.). Proces przeprowadzania audytu to nie tylko kontrola, ale także element wspierający poprawę efektywności organizacji. Regularne przeprowadzanie audytów pozwala na identyfikację potencjalnych ryzyk oraz wdrażanie skutecznych rozwiązań, które mają na celu zapewnienie zgodności działań z przepisami wewnętrznymi organizacji i oczekiwaniami rynku. Ze względu na ciągle zmieniające się przepisy i coraz większe oczekiwania związane z bezpieczeństwem, a także pojawiające się zagrożenia, zaleca się cyklicznie przeprowadzać audyt i na bieżąco weryfikować stosowane zabezpieczenia.

Literatura

1. Akademia Jakości. (b.d.). *Audyt wewnętrzny, Wewnętrzny audyt jakości w przedsiębiorstwie produkcyjnym*, akademijakosci.com. Pobrano z: <https://akademijakosci.com/wewnetrzny-audyt-jakosci-w-przedsiębiorstwie-produkcyjnym> (dostęp: 20.09.2025).
2. Biarda, M. (2022). *Rola audytu w systemach zarządzania, Jakość bez retuszu z Anna Farion*. Pobrano z: <https://jakoscbezretuszu.pl/rola-audytu-w-systemach-zarzadzania> (dostęp: 12.02.2026).
3. Borkowski, T. (b.d.). *Raport z audytu bezpieczeństwa informacji – co powinien zawierać?* Pobrano z: <https://www.pbsg.pl/raport-z-audytu-bezpieczenstwa-informacji/#:~:text=Raport%20z%20audytu%20bezpiecze%C5%84stwa%20informacji%20to%20dokument%2C%20kt%C3%B3ry%20daje%20odpowied%C5%BA,i%20standardy%20dotycz%C4%85ce%20bezpiecze%C5%84stwa%20informacji> (dostęp: 12.02.2026).
4. CeCert. (2024). *Co to jest audyt w firmie? Rodzaje audytów i korzyści z ich przeprowadzenia*, Pobrano z: <https://cecert.pl/co-to-jest-audyt-w-firmie-rodzaje-audytow-i-korzysci-z-ich-przeprowadzenia> (dostęp: 20.09.2025).
5. Delkomtech. (b.d.). *Czym jest audyt bezpieczeństwa informacji i kiedy jest potrzebny w Twojej firmie?* Delkom Group Sp. z o.o. Pobrano z: <https://www.delkomtech.pl/aktualnosci/czym-jest-audyt-bezpieczenstwa-informacji-i-kiedy-jest-potrzebny-w-twojej-firmie> (dostęp: 12.02.2026).
6. EITT. (b.d.). Effective IT Trainings. *Audyt wewnętrzny?* Pobrano z: <https://eitt.pl/slownik/audyt-wewnetrzny> (dostęp: 20.09.2025).
7. EITT. (b.d.). Effective IT Trainings, *Co to jest Audytor bezpieczeństwa informacji?* Pobrano z: <https://eitt.pl/slownik/audytor-bezpieczenstwa-informacji> (dostęp: 21.09.2025).
8. Fehler, W. (2016). *O pojęciu bezpieczeństwa informacyjnego*, W: M. Kubiak, S. Topolewski (red.), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce-Warszawa: Wydawca Pracownia Wydawnicza Wydziału Humanistycznego.
9. Global Cert. (2023). *Cechy dobrego audytora wewnętrznego*. Pobrano z: <https://certyfikacja-iso.pl/2023/10/26/cechy-dobrego-audytora-wewnetrznego> (dostęp: 20.09.2025).

10. Global Cert. (2025). *Norma ISO 19011 – Wytyczne dotyczące audytowania systemów zarządzania*. Pobrano z: <https://certyfikacja-iso.pl/2025/01/17/norma-iso-19011-wytyczne-dotyczace-audytowania-systemow-zarzadzania> (dostęp: 20.09.2025).
11. Godula, M. (2026). *Czym jest Bezpieczeństwo informacji? Definicja, filary, zagrożenia i wdrażanie w organizacji*. Pobrano z: <https://eitt.pl/baza-wiedzy/czym-jest-bezpieczenstwo-informacji-kompedium> (dostęp: 10.03.2026).
12. Qualitywise. (b.d.). *Audyt – nie szukaj niezgodności!*
13. Highspring. (2025). *The top 10 characteristics of exceptional internal audit leaders*, Highspring Jan 29, 2025. Pobrano z: <https://www.highspring.com/blog/the-10-characteristics-of-exceptional-internal-audit-leaders> (dostęp: 20.09.2025).
14. Hotiuk, Z. (2024). *Audyt – narzędzie kontroli czy doskonalenia organizacji?* Pobrano z: <https://pep.pl/poradnik/audyt> (dostęp: 12.02.2026).
15. <https://www.qualitywise.pl/audyt-nie-szukaj-niezgodnosci> (dostęp: 29.09.2025).
16. Instytut Audytorów Wewnętrznych IIA Polska. (b.d.). *Definicja Audyt wewnętrzny*. Pobrano z: <https://www.iaa.org.pl/o-nas/definicia-aw> (dostęp: 21.09.2025).
17. Jurkiewicz, P. (2023). *Jak audyt bezpieczeństwa wygląda w praktyce?* Pobrano z: <https://www.doering-partnerzy.pl/jak-audyt-bezpieczenstwa-wyglada-w-praktyce> (dostęp: 20.09.2025).
18. Klichowski, M. (b.d.). *Na czym polega audyt bezpieczeństwa informacji i dlaczego warto go wykonywać?* Pobrano z: <https://www.pbsg.pl/na-czym-polega-audyt-bezpieczenstwa-informacji> (dostęp: 12.02.2026).
19. Kowalewski, M., Kowalewski J. (2004). *Zarządzanie bezpieczeństwem informacji organizacji*, Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej.
20. Koziej, S. (2011). *Teoria sztuki wojennej*, Warszawa: Wydawnictwo BELLONA.
21. Lean Partner. (b.d.). *Audyt wewnętrzny, Czym jest audyt wewnętrzny? Rodzaje audytów oraz ich cele*. Pobrano z: <https://leanpartner.pl/audyt-wewnetrzny> (dostęp: 20.09.2025).

22. Malon Group. (b.d.). ISO 27001. Wdrożenie ISO 27001 – System Zarządzania Bezpieczeństwem Informacji zgodny z wymaganiami ISO 2700. Pobrano z: <https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/systemy-bezpieczenstwa-informacji/iso-27001> (dostęp: 26.07.2025).
23. Microsoft. (b.d.). *Co to jest bezpieczeństwo informacji?* Pobrano z: <https://www.microsoft.com/pl-pl/security/business/security-101/what-is-information-security-infosec> (dostęp: 12.02.2026).
24. Millichamp, A., Taylor, J. (2018). *Auditing*, 11th Edition, United Kingdom: Cengage Learning EMEA.
25. Ministerstwo Cyfryzacji. (b.d.). *Krajowy system cyberbezpieczeństwa*. Pobrano z: <https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-> (dostęp: 20.09.2025).
26. Moeller, R. (2021). *Nowoczesny audyt wewnętrzny*, Warszawa: Wydawnictwo Nieoczywiste.
27. Nowak, A., Scheffs, W. (2010). *Zarządzanie bezpieczeństwem informacyjnym*. Warszawa: Wydawnictwo AON.
28. Przybylska, J., Rydzak, W., Trębecki, J. (2021). *Skuteczne komunikowanie w audycie wewnętrznym*, Warszawa: Wydawnictwo CeDeWu.
29. PUW. (b.d.). *Czym jest audyt – rodzaje, metody i cele jego przeprowadzania*. Pobrano z: <https://www.puw.pl/pl/strefa-wiedzy/czym-jest-audit-rodzaje-metody-i-cele-jego-przeprowadzania> (dostęp: 20.09.2025).
30. Rada Europejska Rada Unii Europejskiej. (2024) *Ochrona danych w UE*. Pobrano z: <https://www.consilium.europa.eu/pl/policies/data-protection/> (dostęp: 31.08.2025).
31. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Pobrano z: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20120000526> (dostęp: 20.09.2025).
32. Serwis Rzeczypospolitej Polskiej gov.pl. (b.d.). *Standardy Krajowych Ram Interoperacyjności (KRI), Portal Interoperacyjności i Architektury*. Pobrano z: <https://www.gov.pl/web/ia/koncepcja-nowych-kri-dokument> (dostęp: 20.09.2025).

33. Sudhara International. (2023). *ISO 19011:2018 – Co to jest i do czego służy?* Pobrano z: <https://sudharapolska.com/norma-iso-19011/> (dostęp: 12.02.2026).
34. Syta, J. (2025). *Zarządzanie cyberbezpieczeństwem. Pracownicy. Procesy. Technologie*, Warszawa: Wydawnictwo PWN.
35. Urząd Ochrony Danych Osobowych, UODO (2022). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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). Pobrano z: <https://uodo.gov.pl/pl/131/224> (dostęp: 31.08.2025).
36. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560). Pobrano z: <https://www.dziennikustaw.gov.pl/DU/rok/2018/pozycja/1560> (dostęp: 20.09.2025).
37. Widomski, P. (2026). *Co to jest i jak działa Bezpieczeństwo informacji (InfoSec)? – Analiza, Bezpieczeństwo informacji*. Pobrano z: <https://nflo.pl/slownik/bezpieczenstwo-informacji/> (dostęp: 12.02.2026).
38. Wójcik, A. (2017). *Prowadzenie audytu zarządzania bezpieczeństwem organizacyjno-technicznym obiektów (część 2)*. Pobrano z: <https://www.zabezpieczenia.com.pl/ochrona-informacji/prowadzenie-audytu-zarzadzania-bezpieczenstwem-organizacyjno-technicznym-obiektow> (dostęp: 22.09.2025).
39. Wójcik, A. (2019). *Przeprowadzanie audytu zarządzania bezpieczeństwem organizacyjno-technicznym obiektów. Część 6. Prowadzenie audytu. Praktyka i wytyczne*, Pobrano z: <https://www.zabezpieczenia.com.pl/ochrona-informacji/przeprowadzanie-audytu-zarzadzania-bezpieczenstwem-organizacyjno-technicznym-0> (dostęp: 13.02.2026).
40. Wójcik, A. (2017). *Podstawy przeprowadzania audytu dotyczącego zarządzania bezpieczeństwem obiektów*, Zabezpieczenia. Pobrano z: <https://www.zabezpieczenia.com.pl/ochrona-informacji/podstawy-przeprowadzania-audytu-dotyczacego-zarzadzania-bezpieczenstwem-obiektow> (dostęp: 22.09.2025).
41. Zespół LexDigital. (2024). *InfoSec – czyli bezpieczeństwo informacji*. Pobrano z: <https://lexdigital.pl/bezpieczenstwo-informacji> (dostęp: 12.02.2026).