Ewa WOLSKA[1]

AUDYT ZGODNOŚCI Z NORMĄ ISO/IEC 27001: 2005

Streszczenie

Niniejszy artykuł nie jest instrukcją „*Jak przeprowadzić audyt zgodności z normą ISO/IEC 27001*", lecz próbą przybliżenia, czym jest audyt i jakie są etapy jego realizacji, w oparciu o normę ISO 27001. Przeprowadzenie takiego audytu nie jest rzeczą łatwą i wymaga od potencjalnego audytora dobrej znajomości normy i dużej praktyki w zakresie prowadzenia audytów. W poszczególnych rozdziałach starałam się omówić, co to jest audyt, jakie są jego cechy, cele i kryteria oraz jakie działania należy podjąć przy planowaniu i realizacji audytu. Dla podkreślenia korzyści płynących z audytu zgodności z normą ISO 27001 zwróciłam czytelnikowi uwagę na istotne znaczenie podjęcia działań korygujących, które uszczelniają system bezpieczeństwa informacji i są niezwykle ważne w procesie jego doskonalenia.

Abstract

This article is not the instruction "*How to conduct an audit of compliance with ISO/IEC 27001*", but an attempt to approximate what is the audit and what are the stages of its implementation, based on the ISO 27001 standard. Doing of such an audit is not easy and requires a good knowledge from the potential auditor high standards and practices in the conduct of audits. In the individual chapters I have tried to discuss what is auditing, what are its characteristics, objectives and criteria, and what action should be taken when planning and implementing the audit. In to emphasize the benefits of an audit of compliance with ISO 27001. I would turned attention to reader to the importance of taking corrective action to sealing the system information security and are extremely important in the process of improvement.

1 WPROWADZENIE

Bezpieczeństwo informacji jest kwestią niezwykle ważną w kontekście działań biznesowych. Coraz więcej firm skupia się na zapewnieniu bezpieczeństwa ważnych dla organizacji informacji, wprowadzając procedury i polityki bezpieczeństwa w oparciu o przyjęte normy dotyczące tego zakresu. Najczęściej stosowaną normą jest norma ISO/IEC 27001 – Technologia Informacji – Techniki Bezpieczeństwa – System Zarządzania Bezpieczeństwem Informacji – Wymagania. ISO/IEC 27001 jest międzynarodowym standardem systemu zarządzania bezpieczeństwem informacji.

[1] Mgr inż. Ewa Wolska jest wykładowcą w Warszawskiej Wyższej Szkole Informatyki.

Wdrożenie w firmie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w oparciu o normę ISO 27001 pozwala na zachowanie poufności, integralności i dostępności informacji, które stanowią dla organizacji wymierną wartość lub ich ochrona wynika z odpowiednich przepisów prawa.

Skuteczne funkcjonowanie SZBI w organizacji wymaga prowadzenia audytów mających na celu weryfikację poprawności stosowanych zabezpieczeń w odniesieniu do założonych wymagań.

Tematem tego artykułu nie jest omawianie norm dotyczących wdrażania i zarządzania bezpieczeństwem informacji, lecz skupienie się na jednym niezwykle istotnym zagadnieniu związanym z prawidłowym działaniem Systemu Zarządzania Bezpieczeństwem Informacji jakim jest audyt.

2 NORMA ISO/IEC 27001

Norma ISO/IEC 27001:2005 – to norma zawierająca wymagania dla Systemu Zarządzania Bezpieczeństwem Informacji. Norma ta określa wymagania dla ustanowienia, wdrożenia, zarządzania, monitorowania i przeglądu udokumentowanego systemu zarządzania bezpieczeństwem informacji (SZBI) w organizacji.

ISO/IEC 27001 jest międzynarodowym standardem dotyczącym zarządzania bezpieczeństwem informacji wydanym w 2005 r. przez ISO (*International Organization for Standardization*) i Międzynarodowy Komitet Elektrotechniczny (*International Electrotechnical Commission*), opracowanym na podstawie wycofanej już brytyjskiej normy BS7799-2:2002. Istnieją również wydane przez Polski Komitet Normalizacyjny polskie odpowiedniki obu standardów - aktualny PN-ISO/IEC 27001:2007 oraz wycofany PN-I-07799:2005.

Norma ISO/IEC 27001:2005 - Załącznik (A) normatywny zawiera wymagane zabezpieczenia podzielone na 11 obszarów:

1. Polityka bezpieczeństwa
2. Organizacja bezpieczeństwa informacji
3. Zarządzanie aktywami
4. Bezpieczeństwo zasobów ludzkich
5. Bezpieczeństwo fizyczne i środowiskowe
6. Zarządzanie systemami i sieciami
7. Kontrola dostępu
8. Pozyskiwanie, rozwój i utrzymanie systemów informatycznych
9. Zarządzanie incydentami związanymi z bezpieczeństwem informacji
10. Zarządzanie ciągłością działania

11. Zgodność z przepisami prawa

Spełnienie wymagań normy oznacza zastosowanie wszystkich ww. zabezpieczeń.

3 CECHY, KRYTERIA, CEL I RODZAJE AUDYTU ZGODNOŚCI Z NORMĄ ISO 27001

3.1 Co to jest audyt?

Definicja audytu:

Systematyczny, niezależny i udokumentowany proces przeprowadzony w celu uzyskania dowodów z audytu i dokonania ich obiektywnej oceny, aby określić zasięg, w jakim spełnione są kryteria audytu[2].

Powyższej definicja nie tylko opisuje cechy audytu, ale również odnosi się do procesu audytowego, który musi być odpowiednio udokumentowany i przeprowadzony zgodnie z wytyczonymi kryteriami.

3.2 Cechy audytu

- Audyt musi być ***systematyczny*** – oznacza, że warunkiem osiągnięcia maksymalnych korzyści, przy wykorzystaniu dostępnych środków, jest poświęcenie czasu na planowanie, a także metodyczność prowadzenia czynności audytowych i poprawne działania poaudytowe.
- Audyt musi być ***niezależny*** – oznacza, że niezależnie od tego, kto jest odpowiedzialny za jego przeprowadzenie, osoba ta nie może być zależna od osób odpowiedzialnych za stosowanie przyjętych w audytowanym SZBI rozwiązań, a zebrane w czasie audytu dowody muszą być rzetelne i obiektywne.
- Audyt musi być ***udokumentowany*** – oznacza to, że wszystkie czynności audytowe powinny być opisane, a sformułowane niezgodności muszą być podparte zebranymi w czasie audytu dowodami, możliwymi do zweryfikowania.

3.3 Cel audytu

Audyt polega na zbadaniu aktualnego stanu zabezpieczenia zasobów informacyjnych pod względem: poufności, integralności i dostępności, wskazaniu niezgodności oraz

[2] Wg normy ISO 27001

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.

Audyt przeprowadzany jest na poziomie szczegółowości opisanej w ww. normie (nie obejmuje zatem kontroli poprawności konfiguracji sprzętu informatycznego i oprogramowania oraz testów penetracyjnych).

3.4 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:

1) zobowiązania wynikające z zawartych umów,
2) wymagania zawarte w przepisach prawa,
3) politykę firmy oraz dokumenty i procedury opracowane w celu jej wdrożenia,
4) normy (np. ISO/IEC 27001).

3.5 Rodzaje audytów

Istnieją trzy podstawowe rodzaje audytów:

- audyty pierwszej strony (wewnętrzne),
- audyty drugiej strony,
- audyty trzeciej strony.

3.5.1 Audyt pierwszej strony

Audyt pierwszej strony jest audytem wewnętrznym. Prowadzenie audytów pierwszej strony jest nieodłącznym elementem prawidłowego zarządzania bezpieczeństwem informacji. Audyty wewnętrzne są skutecznym sposobem weryfikacji wdrożonych zabezpieczeń w poszczególnych obszarach bezpieczeństwa informacji.

W instytucjach, które wdrożyły System Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001 i zamierzają przeprowadzić procedurę certyfikacyjną, cykliczne wykonywanie audytów wewnętrznych jest wymaganiem obowiązkowym.

3.5.2 Audyt drugiej strony

Audyt drugiej strony polega na audytowaniu dostawców, z którymi instytucja prowadzi działania biznesowe, w oparciu o podpisane umowy.

Norma ISO 27001 nie wymaga audytowania dostawców, jednak znajomość mocnych i słabych punktów dostawcy w zakresie stosowanych zabezpieczeń w celu ochrony przekazywanych mu danych, pomaga organizacji w określeniu potencjalnego ryzyka i wdrożeniu właściwych zabezpieczeń w celu ograniczenia wystąpienia tego ryzyka.

3.5.3 Audyt trzeciej strony

Audyt trzeciej strony jest audytem wykonywanym przez firmę zewnętrzną lub przez niezależną jednostkę certyfikującą.

Audyt trzeciej strony wykonywany przez wykwalifikowanych, niezależnych audytorów z firmy zewnętrznej pozwala w sposób obiektywny sformułować opinię na dotyczącą statusu wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji.

Najczęściej tego typu audyt wykonywany jest wówczas, gdy firma nie zatrudnia osoby posiadającej stosowne kwalifikacje, pozwalające na przeprowadzenie audytu wdrożonych zabezpieczeń w poszczególnych obszarach, w odniesieniu do założonych kryteriów.

Audyt strony trzeciej jest konieczny w sytuacji, gdy instytucja stara się o certyfikat zgodności z normą np. ISO 27001, ISO 9001. Mówimy wówczas o audycie certyfikacyjnym.

4 DZIAŁANIA AUDYTOWE

Właściwie przeprowadzony audyt powinien być zaplanowany i przeprowadzony w sposób bardzo przemyślany. Bardzo istotną kwestią jest dobre zrozumienie celu prowadzonego audytu. Dla ułatwienia sobie zadania należy wykonać cztery działania, określane przez normę jako kluczowe:

1. Planowanie.
2. Wykonywanie.
3. Raportowanie.
4. Działania korygujące i zamknięcie.

4.1 Planowanie audytu

Audyt zawsze pociąga za sobą pewne zakłócenia z działaniu organizacji. Audytor musi jednak mieć dostęp do zasobów i podejmować na miejscu czynności mające czasem

wpływ na normalne funkcjonowanie organizacji. W celu maksymalnego wykorzystania zasobów przy minimalnych zakłóceniach pracy, niezbędne jest właściwe zaplanowanie przebiegu audytu. Dlatego faza planowania jest bardzo istotna dla sprawnego przeprowadzenia audytu. Przed rozpoczęciem właściwych prac audytowych audytor powinien skupić się na przeanalizowaniu celu audytu, założonych kryteriów, a także zasięgu audytu, co pozwoli określić granice, w ramach których prowadzony będzie audyt.

Na etapie planowania dokonywany jest wybór audytora wiodącego, określany skład zespołu audytowego i podział prac audytowych.

Audytor wiodący musi zaplanować również czas potrzebny na wykonanie każdego zadania, jak również czas na spotkania przeglądowe i wymianę informacji pomiędzy członkami zespołu. Niezbędne jest również zaplanowanie spotkań z osobą ze strony audytowanego, odpowiedzialną za przebieg audytu, w celu bieżącego przekazywania informacji odnośnie prowadzonych prac.

W fazie planowania należy wykonać następujące czynności:

1) określić cel i zakres audytu,
2) zebrać informacje użytkowe – liczba i rodzaj zasobów, ilość dokumentów,
3) określić zespół audytowy i wybór kierownika zespołu – audytora wiodącego,
4) określić czas trwania audytu, w tym datę rozpoczęcia (po uzgodnieniu z audytowanym),
5) ustalić kontakt z audytowanym – osoby kontaktowe i formę kontaktu,
6) przygotować plan audytu i harmonogram prac,
7) zorganizować zebranie zespołu audytowego, w celu określenia zadań i roli poszczególnych członków zespołu,
8) przygotować listy kontrolne (ang. *checklist*).

Po opracowaniu planu i harmonogramu audytu należy skonsultować go z audytowanym.

Głównym rezultatem planowania będzie pisemny plan i harmonogram audytu, uzgodniony przez cały zespół audytowy i audytowanego. Harmonogram powinien być przekazany audytowanemu i rozdany członkom zespołu.

4.1.1 Przygotowanie list kontrolnych

Listy kontrolne, tzw. checklisty, to listy pytań odnoszących się do udokumentowanego SZBI i wymagań normy, w określonym dla audytu zakresie. Listy kontrolne są jednym z podstawowych narzędzi roboczych wykorzystywanych podczas audytu.

Celem takiego wykazu jest formalne i szczegółowe planowanie taktyki audytu, osiągnięcie celów audytu (wskazanie niezgodności w SZBI) oraz maksymalne wykorzystanie zasobów audytu (zespołu).

Przygotowanie skutecznej listy kontrolnej wymaga wysiłku i poświęcenia sporej ilości czasu. Nie ma idealnego wzoru, który pozwoliłby na przygotowanie skutecznej listy kontrolnej. Każdy audytor musi przygotować listy odpowiednio dostosowane do audytu, wykorzystując dostępne mu źródła, jakimi są:

1) cel i zakres audytu,
2) raporty z poprzednich audytów,
3) udokumentowany System Zarządzania Bezpieczeństwem Informacji,
4) normy, specyfikacje odpowiadające bezpieczeństwu informacji w obrębie zakresu audytu,
5) wymagania normy ISO 27001.

Lista kontrolna powinna być tak zaprojektowana, aby „poprowadzić" audytora poprzez dobrze zaplanowany i logiczny ciąg zdarzeń. Podczas projektowania takiej listy audytor musi skupić się na zrozumieniu zaplanowanej strategii audytu, uwzględniającej działy, obszary pracy, zakresy odpowiedzialności, wymagania SZBI. Oznacza to, że przy sporządzaniu jej należy wziąć pod uwagę specyfikę firmy i funkcje audytowanych działów, ich odpowiedzialność za realizację zadań zgodnie z funkcjonującym systemem zarządzania bezpieczeństwem informacji, a także obszary, które podlegają badaniu.

Jedną ze znanych technik sporządzania list kontrolnych jest zadawanie pytań: „co?" i „dlaczego?", np.:

1. *Co muszę wiedzieć? Dlaczego muszę to wiedzieć?*
2. *Co muszę sprawdzić? Dlaczego muszę to sprawdzić?*
3. *Jakie próbki muszę zobaczyć? Dlaczego muszę je zobaczyć?*

Dobrze sporządzone listy kontrolne pomagają audytorowi, dlatego warto jest przy ich sporządzaniu oszacować czas potrzebny na udzielenie odpowiedzi i zebranie próbek, a także dodać odnośniki do dokumentów, które stymulowały pytania.

4.1.2 Rodzaje list kontrolnych

Najczęściej stosowane rodzaje list kontrolnych to listy kryteriów i audytu. W fazie przygotowania do audytu sporządzamy obydwa rodzaje.

Poniżej krótka charakterystyka obydwu rodzajów list kontrolnych:

1) lista kryteriów – zawiera bardzo obszerne pytania zamknięte (odpowiedź „tak" lub „nie"), które mają być pomocne w określeniu wszelkich głównych zaniedbań w audytowanym systemie,

2) lista audytu – szczegółowe pytania odnoszące się do audytowanego systemu, sporządzone w oparciu o dostępne źródła oraz listy stosowanych kryteriów.

4.2 Wykonywanie audytu

4.2.1 Spotkanie otwierające

Niezwykle ważną kwestią, od której rozpoczyna się właściwy audyt w siedzibie audytowanego, jest spotkanie otwierające. Głównym celem spotkania otwierającego jest przedstawienie zespołu audytowego przedstawicielom audytowanej organizacji i upewnienie się, że audytowany rozumie cel audytu i ogólne zasady oceny.

Na spotkanie otwierającym, oprócz potwierdzenia zakresu audytu i przedstawienia metodyki jego prowadzenia, są omówione również kwestie organizacyjne i techniczne związane z przebiegiem audytu.

Przebieg spotkanie otwierającego:

1. Przedstawienie zespołu audytowego.
2. Ponowne przedstawienie celu audytu i zatwierdzenie go przez audytowanego.
3. Ponowne potwierdzenie zakresu audytu.
4. Przedstawienie metodyki audytu.
5. Przedstawienia planu audytu i harmonogramu prac audytowych.
6. Ustalenie osób ze strony firmy audytowanej biorących udział w audycie (udzielających odpowiedzi na pytania, dostarczających dokumenty, odpowiedzialnych za logistykę).
7. Potwierdzenie zasad poufności.
8. Przedstawienie metody raportowania.
9. Odpowiedzi na pytania ze strony audytowanego.
10. Zamknięcie spotkania otwierającego.

4.2.2 Prace audytowe

Prace audytowe, rozdzielone przez audytora wiodącego w fazie planowania, prowadzone są przez członków zespołu, zgodnie z założonym harmonogramem. Jeżeli pojawia się potrzeba audytowania poza przypisanym zadaniem, audytor wiodący musi być o tym poinformowany. Każdy z audytorów prowadzi audyt indywidualnie, w towarzystwie przydzielonej mu osoby, tzw. przewodnika, ze strony audytowanego. Wymiana infor-

macji pomiędzy członkami zespołu następuje na założonych z góry i uwzględnionych w harmonogramie, zebraniach audytorów.

Prace audytowe przeprowadzane są metodą próbkowania, w oparciu o przygotowane listy kontrolne. Oznacza to, że nie jest szczegółowo badany cały obszar, lecz wybrane jego elementy. Próbki powinny być potwierdzone dowodami z uwagi na to, że na etapie raportowania, posłużą do sformułowania wykrytych niezgodności.

W celu uzupełnienia informacji audytor przeprowadza wywiady z wybranymi użytkownikami systemu informacyjnego. Audytor powinien poinformować kierownika działu, że będzie prowadził wywiady w kierowanym przez niego obszarze. Następnie, kierując się listą kontrolną, systematycznie zbiera informacje i sprawdza, czy konieczne zabezpieczenie zostały określone i poprawnie wdrożone. Audytor powinien przestrzegać zasady zadawania tylko jednego pytania na raz.

Dodatkowym źródłem informacji o systemie zarządzania bezpieczeństwem informacji są wizje lokalne w siedzibie audytowanego. Przeprowadzenie wizji lokalnych pozwala na pełniejsze opisanie funkcjonującego SZBI.

Zakres prac audytowych obejmuje:

1) analizę istniejących w firmie dokumentów: procedur, instrukcji, regulaminów dotyczących bezpieczeństwa informacji, wchodzących w skład Polityki Bezpieczeństwa;
2) ocenę ww. dokumentów pod kątem zgodności z normą ISO/IEC 27001:2005, w oparciu o Załącznik A tej normy;
3) weryfikację poprawności wdrożenia i funkcjonowania opisanych zabezpieczeń – wywiady z użytkownikami systemu i wizje lokalne;
4) weryfikację poprawności realizacji procedur, zawartych w Polityce Bezpieczeństwa – wywiady z pracownikami odpowiedzialnymi za realizację procedur.
5) opracowanie raportu z audytu – opis funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji w odniesieniu do wytycznych zawartych w normie, sformułowanie niezgodności i rekomendacji.

4.3 Raportowanie

Wyniki audytu przedstawiane są w formie raportu z audytu. Odbiorcą raportu jest zwykle Zarząd organizacji, w której audyt był prowadzony, dlatego zapisy w raporcie powinny być jasne i zrozumiałe dla odbiorcy. Sformułowane w raporcie niezgodności powinny być poparte dowodami i odnosić się do punktów normy.

4.3.1 Opis niezgodności

Termin *niezgodność* używany jest przez normę ISO/IEC 27001 do określenia braku spełnienia wymagania.

Identyfikacja niezgodności musi być poparta dowodem, czyli danymi świadczącymi o jej istnieniu. Dowody mogą być zdobyte przez pomiar, testy, udzielone odpowiedzi audytowanych, obserwacje audytorów, zapisy lub ich brak w dokumentach oraz inne środki.

Celem dokumentowania niezgodności jest zdefiniowanie skutecznych działań korygujących. Punktem wyjściowym do działań korygujących, realizowanych na podstawie zawartych w raporcie zaleceń, jest dobre zrozumienie problemu. Dobrze sformułowany opis niezgodności może być pomocny w określeniu efektu występującego problemu i wskazaniu jego przyczyny. To z kolei znacznie ułatwi dobór zabezpieczeń w celu usunięcia problemu lub zmniejszenia ryzyka jego ponownego wystąpienia.

Opis niezgodności opiera się na porównaniu:

1) zdefiniowanego systemu zarządzania bezpieczeństwem informacji z narzuconymi wymaganiami,
2) wdrożonego systemu (SZBI) ze zdefiniowanym systemem (SZBI),
3) danych wyjściowych SZBI z wymaganiami.

Niezgodność wynikająca z porównania zdefiniowanego SZBI z narzuconymi wymaganiami ma miejsce wówczas, gdy nie został zdefiniowany przez audytowanego mechanizm, poprzez który można osiągnąć wymagania zawarte w przepisach prawa i normie oraz wynikające z umów i polityki firmy.

Niezgodność wynikająca z porównania zawartego w punkcie 2 występuje wówczas, gdy audytowany zdefiniował mechanizm i określił procedury, ale się do nich nie stosuje.

Niezgodność wynikająca z porównania opisanego w punkcie 3 występuje wtedy, kiedy nie są spełnione wymagania, pomimo tego, że mechanizm jest zdefiniowany, a procedury są przestrzegane. Oznacza to, że system w badanym obszarze nie jest skuteczny.

W momencie, gdy audytor stwierdzi, że istnieją wystarczające przesłanki do stwierdzenia niezgodności (tzn. zebrał dowody na istnienie niezgodności) powinien poinformować o tym audytowanego. Audytor nie powinien ukrywać swoich obserwacji i obaw wynikających z wykrytych niezgodności aż do zakończenia audytu. Po uzgodnieniu faktów audytowany powinien dowiedzieć się o zapisaniu niezgodności. Wszystkie zidentyfikowane niezgodności powinny być omówione z audytowanym i przez niego podpisane. Takie podejście świadczy o rzetelności audytora.

Opis niezgodności powinien być zwięzły, konkretny i poparty dowodami. Z jednej strony musi być na tyle obszerny, aby zawarte były w nim wszystkie istotne fakty i oko-

liczności odkrycia niezgodności, a z drugiej strony na tyle krótki, jak to tylko jest możliwe.

Przy opisywaniu niezgodności, w celu utrzymania dokładności i zwięzłości, należy rozpatrzyć następujące kwestie:

1) *gdzie zaobserwowano niezgodność?* – wskazanie miejsca pozwoli na podjęcie działań prewencyjnych lub natychmiastowych działań korygujących, zależnie od skali wykrytej niezgodności
2) *jakie obserwacje zdecydowały o odkryciu niezgodności?* – określenie przedmiotu problemu
3) *dlaczego jest to niezgodnością?* – odniesienie do naruszonego wymagania
4) *kogo niezgodność dotyczyła?* – czasami niezbędna jest identyfikacja osoby (nie koniecznie imienia i nazwiska, raczej stanowiska lub funkcji), która jest odpowiedzialna za obszar, w którym niezgodność odkryto, w celu weryfikacji zakresów odpowiedzialności określonych w ramach wdrożonego SZBI.

Każda zapisana niezgodność powinna być oceniona w przyjętej przez audytora skali. Norma ISO 27001 nie definiuje skali jaką powinien posługiwać się audytor przy klasyfikowaniu niezgodności. Klasyfikacja przyjęta przez audytora powinna być jednak jasna i jednoznaczna.

Z praktyki wynika, że optymalną skalą do klasyfikacji niezgodności jest określenie poziomu zgodności w skali trzystopniowej. Najwygodniej poziom zgodności opisać cyframi 1, 2, 3 lub literami A, B, C, przy czym 1(A) - niezgodność mała, 2 (B) – niezgodność średnia, 3 (C) – niezgodność duża.

W momencie określania poziomu zgodności dla sformułowanej niezgodności należy rozważyć jak duże konsekwencje będzie miała ta niezgodność na system zarządzania bezpieczeństwem informacji, jeżeli nie zostanie poprawiona, jakie jest prawdopodobieństwo wystąpienia tych konsekwencji oraz jak szybko i przy jakim wysiłku niezgodność może być usunięta.

Niezależnie od przyjętej konwencji klasyfikacji zespół audytowy zawsze musi umieć ocenić, czy wykryta niezgodność jest poważna i trudna do usunięcia, czy mała i nie pociąga za sobą zasadniczej zmiany systemu zarządzania bezpieczeństwem informacji.

4.3.2 Raport z audytu

Raport z audytu powinien zawierać ocenę zgodności funkcjonującego w organizacji systemu zarządzania bezpieczeństwem informacji w odniesieniu do wymagań zawartych w normie ISO 27001.

Ocena zgodności przedstawiana jest opisowo i zawiera informację na temat sposobu spełnienia wymagania, bądź informację o jego niespełnieniu - niezgodność wraz z oceną stopnia niezgodności - mała - 1, średnia - 2, duża - 3.

Raport z audytu powinien zawierać w szczególności:

1) szczegóły dotyczące audytowanego,
2) cel i zakres (obszary) audytu,
3) stosowaną normę,
4) opis metodyki audytu,
5) imiona i nazwiska audytorów,
6) ustalenia (próbki) oraz dowody tych ustaleń,
7) listy kontrolne,
8) sformułowane niezgodności wraz ze wskazaniem punktów normy, w których te niezgodności występują,
9) rekomendacje do działań korygujących.

Kompletny raport powinien przekazany w ustalonym z audytowanym terminie. Audytowany ma prawo wnieść zastrzeżenia i uwagi do raportu. W takim przypadku audytor wiodący musi odnieść się do przekazanych uwag i zastrzeżeń. Często uzgodnienie stanowisk jest bardzo trudne i wymaga dużego wysiłku i rzetelnych dowodów ze strony audytora. Po uzgodnieniu spornych zapisów raport jest przez obie strony ratyfikowany. Raport jest dokumentem aktywnym, aż do momentu usunięcia wszystkich wskazanych w nim niezgodności.

Należy pamiętać, że informacje zawarte w raporcie są informacjami wrażliwymi, których ujawnienie mogłoby przynieść szkodę audytowanemu. W związku z tym raport jest dokumentem poufnym, któremu musi być zapewnione również bezpieczeństwo fizyczne.

4.4 Działania korygujące i zamknięcie

Po zakończeniu prac audytowych audytor wiodący organizuje spotkanie zespołu, omawiane są wszystkie zidentyfikowane niezgodności i przygotowany raport podsumowujący audyt. Celem przygotowania raportu podsumowującego jest zebranie wszystkich faktów razem tak, aby na spotkaniu zamykającym mogły być zaprezentowane audytowanemu. Raport podsumowujący powinien zawierać wyraźną interpretację faktów, aby przedstawić audytowanemu wnioski z audytu i upewnić się, że są one dla niego zrozumiałe.

4.4.1 Spotkanie zamykające

Spotkanie zamykające jest spotkaniem formalnym, które odbywa się według określonego planu. Omówienie prac audytowych i przedstawienie raportu podsumowującego należy do audytora wiodącego.

Typowy program spotkania zamykającego wygląda w następujący sposób:

1. Lista uczestników – wyznaczony przez audytora wiodącego członek zespołu audytowego sporządza listę uczestników spotkania.
2. Podziękowania ze strony audytorów za pomoc okazaną przez audytowanych w trakcie prowadzonego audytu.
3. Przypomnienie celu i zakresu audytu – nie można zakładać, że wszystkie obecne na spotkaniu zamykającym osoby, uczestniczyły w spotkaniu otwierającym i znają cel i zakres prowadzonego audytu.
4. Omówienie sposobu raportowania – potwierdzenie, że podpisane przez obie strony kopie niezgodności zostaną przekazane po spotkaniu, a kompletny raport zostanie przesłany w umówionym terminie.
5. Wskazanie ograniczeń – audytor wiodący potwierdza, że audyt prowadzony był w określonym zakresie i nie powstała żadna ocena dotycząca czynności znajdujących się poza zakresem audytu, podkreśla również, że audyt prowadzony był metoda próbkowania, co może oznaczać, iż nie wszystkie niezgodności zostały wykryte oraz nie można zagwarantować prawdziwości zidentyfikowanych niezgodności, mimo rzetelności audytorów.
6. Przedstawienie niezgodności – każdy z audytorów przedstawi zidentyfikowane przez siebie niezgodności.
7. Podsumowanie prac audytowych – przedstawienie wniosków i zaleceń opartych na całym audycie, opisanych w raporcie podsumowującym.
8. Wyjaśnienia – audytowany ma prawo do uzyskania wyjaśnień odnośnie wszystkich aspektów audytu, zadaje pytania audytorom i prosi o wyjaśnienie niezrozumiałych kwestii.
9. Uzgodnienia – audytowany podejmuje zobowiązania do wprowadzenia działań korygujących, w przypadku, gdy prowadzony audyt był audytem certyfikacyjnym, audytowany określa termin zakończenia działań korygujących.
10. Pożegnanie.

4.4.2 Działania korygujące

Wiele audytów jest nieskutecznych z powodu niepodjęcia ze strony audytowanego działań korygujących. W większości przypadków podczas audytu zapisywana jest więcej niż jedna niezgodność, która określa skutki problemu. Audytowany powinien zbadać przyczynę problemu i wdrożyć działania korygujące w celu jej likwidacji lub zmniejszenia ryzyka ponownego wystąpienia problemu.

W przypadku audytów trzeciej strony, czyli audytów certyfikacyjnych zgodności wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji z normą ISO/IEC 27001:2005, audytor może poprosić audytowanego o program działań korygujących, niezawierający jedynie tych niezgodności, które zostały poprawione w trakcie audytu. Program powinien uwzględniać przedziały czasowe, w jakich zadania korygujące zostaną podjęte i zakończone. Audytor powinien natomiast sprawdzić, czy w uzgodnionym czasie niezgodności zostały usunięte lub czy harmonogram uwzględnia jakieś zmiany i przyczyny tych zmian, w przypadku ich nieusunięcia.

W przypadku niezgodności zaklasyfikowanych jako „małe" i „średnie", ocena dotycząca ich usunięcia nie wymaga ponownej wizyty audytorów. Wystarczająca jest odpowiedź audytowanego odnośnie sposobu usunięcia niezgodności. Weryfikacja podjętych działań nastąpi wówczas podczas pierwszej rutynowej wizyty audytorów, w trakcie ważności certyfikatu. W przypadku „dużych" niezgodności, sposób ich usunięcia podlega ocenie w trakcie wizyty pokontrolnej, przed wydaniem certyfikatu.

5 PODSUMOWANIE

Audyty systemu zarządzania bezpieczeństwem informacji przeprowadzone przez kompetentnych audytorów mają wiele korzyści dla audytowanego. Do najważniejszych należą:

1) sprawdzenie zastosowania, zgodności i skuteczności systemu,
2) wprowadzenie odpowiednich zmian, wynikających z wykrytych niedoskonałości systemu,
3) wskazanie audytorowi wewnętrznemu i osobom odpowiedzialnym za realizację procedur i polityk bezpieczeństwa możliwości dalszego doskonalenia systemu, poprzez podejmowanie działań prewencyjnych,
4) znajomość słabych punktów naszych dostawców – w przypadku audytów drugiej strony.

Ostatecznym celem audytów jest udoskonalenie Systemu Bezpieczeństwa Informacji. Dlatego ostatnim zadaniem audytu są czynności poaudytowe, które trwają do czasu

sprawdzenia efektywności podjętych działań korygujących. Audyt może być nieskuteczny, jeżeli jego rezultatem nie będzie podjęcie działań korygujących.

Literatura

1. Międzynarodowa Norma ISO/IEC 27001:2005 – Technologia informacji – Techniki Bezpieczeństwa – Systemy Zarządzania Bezpieczeństwem Informacji – Wymagania.
2. Polska Norma PN-ISO/IEC 17799:2005 – Technika informatyczna – Techniki Bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.
3. Raport Techniczny ISO/IEC TR 13335-3:1998 – Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych.
4. Materiały szkoleniowe z kursu dla audytorów wiodących ISO/IEC 27001, wyd. Excel Partnership, 2006.