CERTYFIKACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI ISMS Z WYKORZYSTANIEM KOMPUTEROWO WSPOMAGANYCH TECHNIK AUDITOWANIA CAAT

Monika STOMA, Agnieszka DUDZIAK, Wiesław PIEKARSKI

Streszczenie: W pracy zaprezentowano możliwość wykorzystania wspomaganych komputerowo technik auditowania CAAT (Computer Assisted Auditing Techniques) przez jednostki certyfikujące systemy zarządzania w odniesieniu do certyfikacji systemu zarządzania bezpieczeństwem informacji. Określono ponadto zakres w jakim istnieje możliwość zastosowania CAAT podczas certyfikacji systemu zarządzania bezpieczeństwem informacji ISMS.

Słowa kluczowe: systemy zarządzania, zarządzanie bezpieczeństwem informacji ISMS, wspomagane komputerowo techniki auditowania, certyfikacja, audit, jednostki certyfikujące.

1. Certyfikacja systemu zarządzania bezpieczeństwem informacji ISMS

Wymagania, jakie powinna spełniać organizacja ubiegająca się o certyfikację systemu zarządzania bezpieczeństwem informacji ISMS, określone są w normie PN-ISO/IEC 27001:2007. Jednostki certyfikujące zalecają, aby organizacja ubiegająca się o certyfikację systemu zarządzania bezpieczeństwem informacji ISMS oprócz w/w wymagań przeprowadzała również tzw. działania systemowe, czyli: audity wewnętrzne w całym zakresie funkcjonowania systemu zarządzania bezpieczeństwem informacji, przeglądy systemu zarządzania bezpieczeństwem informacji oraz działania korygujące i zapobiegawcze. Większość jednostek certyfikujących nie udziela certyfikacji dopóki nie uzyska wystarczającego dowodu na to, że ustalenia dotyczące auditów wewnętrznych i przeglądów zarządzania zostały wdrożone, są skuteczne i są utrzymywane.

Współpraca pomiędzy jednostką certyfikującą ISMS a organizacją wnioskującą o certyfikację rozpoczyna się z chwilą złożenia przez wnioskującą organizację wniosku o certyfikację ISMS. Jednostka certyfikująca dokonuje oceny wniosku o certyfikację ISMS [11], a następnie wyznacza zespół auditujący. Zespół auditujący powinien być kompetentny w odniesieniu do danej branży wg Polskiej Klasyfikacji Usług[9], w której przeprowadzać będzie certyfikację ISMS [6]. Skład zespołu auditującego powinien zostać zaakceptowany przez auditowaną organizację.

Jednym z najważniejszych zagadnień związanych z oceną wniosku o certyfikację jest ustalenie czasu niezbędnego do oceny ISMS. Głównym parametrem determinującym czas niezbędny do przeprowadzenia oceny jest liczba pracowników certyfikowanej organizacji (tab.1) [8]. Zasady wyznaczania czasu pracy zespołu auditującego są spójne dla wszystkich systemów zarządzania [4]. Certyfikacja ISMS udzielana jest na podstawie pozytywnego wyniku auditu certyfikacyjnego na okres trzech lat. W ciągu trzech lat certyfikowana

organizacja zobowiązana jest poddać się dwóm auditom nadzoru. Audit certyfikacyjny ISMS przeprowadzany jest w dwóch etapach [6].

Tab. 1. Czas oceny dla auditu certyfikacyjnego systemu zarządzania bezpieczeństwem informacji ISMS.

Liczba pracowników	Czas pracy auditorów podczas oceny w procesie certyfikacji (liczba auditorodni)
1 - 10	5
11 - 25	7
26 - 45	8,5
46 - 65	10
66 - 85	11
86 - 125	12
126 - 175	13
176 - 275	14
276 - 425	15
426 - 625	16,5
626 - 875	17,5
876 - 1175	18,5
1176 - 1550	19,5
1551 - 2025	21
2026 - 2675	22
2676 - 3450	23
3451 - 4350	24
4351 - 5450	25
5451 - 6800	26
6801 8500	27
8501 - 10700	28
> 10700	Według powyższej tendencji

Źródło: Załącznik B do normy PN-EN/IEC 27006:2009 [8]

Pierwszy etap auditu certyfikacyjnego ISMS jednostka certyfikująca prowadza w celu:

- oceny dokumentacji ISMS, a w szczególności analizy ryzyka związanego z bezpieczeństwem informacji oraz deklaracji stosowania,
- weryfikacji wszystkich lokalizacji klienta i specyficznych dla lokalizacji warunków,
- przeglądu statusu klienta i zrozumienia przez niego wymagań ISMS, zwłaszcza w odniesieniu do identyfikacji zagrożeń i analizy ryzyka,
- zebrania niezbędnych informacji dotyczących zakresu systemu zarządzania i prawnych aspektów związanych z bezpieczeństwem informacji,
- przeprowadzenia dyskusji z personelem klienta w celu określenia gotowości do drugiego etapu auditu certyfikacyjnego,
- przeprowadzenia przeglądu przydziału zasobów do drugiego etapu auditu certyfikacyjnego i uzgodnienia z klientem szczegółów z tym związanych,
- zaplanowania etapu drugiego auditu certyfikacyjnego,
- oceny, czy są planowane i realizowane audity wewnętrzne i przeglądy zarządzania, oraz czy poziom wdrożenia systemu zarządzania uzasadnia gotowość klienta do certyfikacji.

Jednostki certyfikujące pierwszy etap lub część pierwszego etapu przeprowadzają w siedzibie certyfikowanej organizacji[10]. Pierwszy etap auditu certyfikacyjnego kończy

się przekazaniem uwag od zespołu auditującego ISMS auditowanej organizacji oraz ustaleniem terminu przeprowadzenia drugiego etapu auditu certyfikacyjnego.

Drugi etap auditu certyfikacyjnego ISMS poprzedzony jest planem auditu przygotowanym przez osobę zarządzającą auditem i członkami zespołu auditującego – auditora wiodącego. Drugi etap auditu certyfikującego ISMS jest auditem przeprowadzanym na miejscu w organizacji, podczas którego zbierane są dowody zgodności systemu zarządzania bezpieczeństwem informacji z normą PN-ISO/IEC 27001:2007 [7].

Celem drugiego etapu auditu certyfikacyjnego jest ocena stopnia wdrożenia ISMS, w tym skuteczności funkcjonującego ISMS. Drugi etap auditu certyfikacyjnego obejmuje:

- informacje i dowody zgodności ze wszystkimi wymaganiami ISMS,
- monitorowanie, pomiary, raportowanie i przeglądanie osiągnięć w odniesieniu do kluczowych celów i zadań,
- zakres zgodności ISMS z wymaganiami prawnymi,
- kontrolę operacyjną ISMS,
- audity wewnętrzne i przeglądy zarządzania ISMS,
- odpowiedzialność kierownictwa oraz polityki certyfikowanej organizacji,
- powiązania pomiędzy wymaganiami normatywnymi, polityką, celami i zadaniami dotyczącymi osiągnięć, wszystkimi mającymi zastosowanie wymaganiami prawnymi, odpowiedzialnością, kompetencjami personelu, działaniami, procedurami, danymi dotyczącymi osiągnięć oraz ustaleniami i wnioskami z auditów wewnętrznych i przeglądów ISMS.

Ponadto zespół auditujący powinien zwrócić uwagę na następujące elementy:

- czy organizacja potrafi wykazać, że analiza zagrożeń bezpieczeństwa informacji ma związek z działalnością organizacji i jest do niej adekwatna,
- czy organizacja dokonała oceny zgodności z prawem i przepisami oraz, że podjęła działania w przypadku stwierdzenia niezgodności z odpowiednimi przepisami.

Po zakończeniu drugiego etapu auditu certyfikacyjnego auditor wiodący opracowuje raport z auditu, na podstawie którego jednostka certyfikując podejmuje decyzję o certyfikacji ISMS.

Jak już wspomniano, w trzyletnim cyklu certyfikacji jednostka certyfikująca przeprowadza dwa audity kontrolne, tzw. audity w nadzorze. Celami auditu nadzoru są: sprawdzenie, czy zaaprobowany system zarządzania bezpieczeństwem informacji ISMS nadal funkcjonuje, oraz, czy nie wystąpiły zmiany w tym systemie mające wpływ na jego funkcjonowanie oraz potwierdzenie stałej zgodności z wymaganiami stawianymi przy certyfikacji ISMS.

Każdy audit nadzoru powinien obejmować:

- ocenę skuteczności ISMS w odniesieniu do osiągania celów polityki organizacji w zakresie bezpieczeństwa informacji,
- ocenę funkcjonowania procedur okresowej oceny i przeglądu zgodności z odnośnymi przepisami i regulacjami dotyczącymi bezpieczeństwa informacji,
- przegląd działań mających na celu usunięcie niezgodności stwierdzonych podczas ostatniego auditu,
- weryfikację elementów utrzymania systemu, którymi są audity wewnętrzne, przeglądy zarządzania oraz działania korygujące i zapobiegawcze,
- ocenę zmian w udokumentowanym systemie,
- badanie obszarów, które podlegały zmianom,

- wykorzystywanie certyfikatu oraz stosowanie znaków certyfikacji ISMS,
- jeżeli wystąpiły, to ocenę zapisów z odwołań, skarg i spraw spornych wnoszonych do jednostki certyfikującej, oraz zapisy świadczące o tym, że w przypadku wykrycia jakiejkolwiek niezgodności lub naruszenia wymagań certyfikacji, organizacja prześledziła własne systemy i procedury i wykonała odpowiednie działania korygujące.

Audity nadzoru ISMS kończą się sporządzeniem przez auditora wiodącego raportu. Po zakończeniu trzyletniego cyklu certyfikacji ISMS certyfikowana organizacja może ubiegać się o ponowną certyfikację na kolejne trzy lata.

2. Certyfikacja systemu zarządzania bezpieczeństwem informacji ISMS z wykorzystaniem wspomaganych komputerowo technik auditowania CAAT

W związku z nieustannym rozwojem technik informatycznych oraz teleinformatycznych powstaje pytanie, czy jest możliwe, a jeżeli tak, to w jakim stopniu, zastosowanie technik komputerowych do oceny systemu zarządzania bezpieczeństwem informacji ISMS? [12]

Ramy do przeprowadzenia analizy zastosowania CAAT podczas certyfikacji ISMS określają następujące międzynarodowe standardy:

- PN-ISO/IEC 27006:2009 Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji [8];
- PN-EN ISO/IEC 17021:2006 Ocena zgodności. Wymagania dla jednostek prowadzących auditowania i certyfikację systemów zarządzania [6];
- PN-EN ISO 19011:2003 Wytyczne dotyczące auditowania systemów zarządzania jakością i/lub zarządzania środowiskowego [5],
- IAF MD 3:2008; Dokument obowiązkowy International Accreditation Forum dotyczący zaawansowanych procedur nadzoru i ponownej certyfikacji [2];
- IAF MD 4:2008; Dokument obowiązkowy International Accreditation Forum dotyczący stosowania wspomaganych komputerowo technik auditowania CAAT w akredytowanej certyfikacji systemów zarządzania [3].

Do podstawowych wspomaganych komputerowo technik auditowania CAAT można zaliczyć:

- telekonferencje,
- spotkania internetowe,
- komunikację interaktywną przy zastosowaniu sieci internetowej,
- zdalny dostęp elektroniczny do dokumentacji,
- zdalny dostęp do procesów systemu zarządzania,
- zdalny dostęp do zasobów certyfikowanej organizacji.

Podstawowym problemem, jaki występuje podczas przeprowadzania auditów CAAT w odniesieniu do systemów zarządzania są kompetencje zespołu auditującego, traktowane jako zdolność auditorów do rozumienia oraz do wykorzystywania technologii informatycznych [3]. W przypadku systemu zarządzania bezpieczeństwem informacji ISMS jednostka certyfikująca nie powinna mieć problemów ze spełnieniem tego wymagania, ponieważ zespół auditujący ISMS musi posiadać wysokie kompetencje w zakresie technologii informatycznych.

Kolejnym elementem przemawiającym za zastosowaniem CAAT w certyfikacji ISMS, jest fakt, iż niektóre z zabezpieczeń wymaganych w systemie zarządzania bezpieczeństwem informacji ISMS muszą zostać przetestowane przez zespół auditujący podczas auditu [8]. Jednocześnie zastosowanie CAAT powoduje skrócenie czasu auditu w organizacji o 30% [3] czasu auditu założonego przez jednostkę certyfikującą dla danej organizacji (tab. 1), tak więc np. audit certyfikacyjny ISMS zaplanowany dla organizacji zatrudniającej 20 osób wynosi 7 auditoro-dni. Po zastosowaniu zasad CAAT audit na miejscu w organizacji wyniósłby 4,9 auditoro-dnia, natomiast pozostałe 2,1 auditoro-dnia można przeprowadzić zdalnie. Przykładowy Obszar wymagań oraz zabezpieczeń, które mogą zostać objęte auditem CAAT przedstawiono w tab. 2.

Tab. 2. Wymagania dla auditu ISMS technikami klasycznymi z rozszerzeniem o zasady CAAT.

Wymagania i zabezpieczenia wg PN-ISO/IEC 27001:2007	Klasyczny audit ISMS			Możliwości zastosowania CAAT podczas auditu ISMS	
	Zabezpieczenia	Testowanie systemu	Kontrola wzrokowa	Badanie auditowi CAAT	Testowanie za pomocą CAAT
4 System zarządzania bezpieczeństwem informacji ISMS	organizacyjne				
4.2 Ustanowienie i zarządzanie ISMS	organizacyjne		zarządzenia		
4.3 Wymagania dotyczące dokumentacji	organizacyjne		procedury, wykaz zapisów		
5 Odpowiedzialność kierownictwa	organizacyjne		zarządzenia		
5.1 Zaangażowanie kierownictwa	organizacyjne				
5.2 Zarządzanie zasobami	organizacyjne		akta osobowe		
6 Wewnętrzne audity ISMS	organizacyjne		plany i raporty z auditów ISMS	ocena raportów z auditów ISMS	
7 Przeglądy ISMS realizowane przez kierownictwo	organizacyjne		raporty z przeglądu ISMS	ocena raportów z przeglądu ISMS	
8 Doskonalenie ISMS	organizacyjne		ocena ISMS		
8.1 Ciągłe doskonalenie ISMS	organizacyjne		zapisy z doskonalenia ISMS		
8.2 Działania korygujące	organizacyjne		karty działań korygujących	badanie przebiegu działań korygujących	zgłoszenie reklamacji
8.3 Działania zapobiegawcze	organizacyjne		karty działań zapobiega-wczych	badanie przebiegu działań zapobiega-wczych	
A5.1 Polityka bezpieczeństwa informacji	organizacyjne		protokoły z przeglądu zarządzania	badanie protokołów z przeglądu zarządzania	
A6.1 Organizacja zewnętrzna	organizacyjne		kopie umów o zachowaniu poufności	badanie protokołów z zebrań kierownictwa	
A6.2 Strony zewnętrzne	organizacyjne		sprawdzenie warunków umów ze stronami zewnętrznymi		
A7.1 Odpowiedzialność za aktywa	organizacyjne		zdefiniowanie aktywów		
A7.2 Klasyfikacja	organizacyjne		oznaczenie		oznaczenie

informacji			i postępowanie z informacjami		wiadomości i przesyłanych plików
A8.1 Przed zatrudnieniem	organizacyjne		zasady i warunki zatrudnienia		
A8.2 Podczas zatrudnienia	organizacyjne		uświadomienie, kształcenie i szkolenie z zakresu bezpieczeństwa informacji		
A8.3 Zakończenie lub zmiana zatrudnienia	organizacyjne i techniczne	odebranie praw dostępu	zwrot aktywów		
A9.1 Obszary bezpieczne	organizacyjne i techniczne		fizyczne zabezpieczenie wejścia		
A9.2 Bezpieczeństwo sprzętu	organizacyjne i techniczne		lokalizacja sprzętu		
A10.1 Procedury eksploatacyjne i zakresy odpowiedzialności	organizacyjne i techniczne	zarządzanie zmianami			
A10.2 Zarządzanie usługami dostarczonymi przez strony trzecie	organizacyjne i techniczne	monitorowanie i przegląd usług strony trzeciej			
A10.3 Planowanie i odbiór systemów	organizacyjne i techniczne	zarządzanie pojemnością			
A10.4 Ochrona przed kodem złośliwym i kodem mobilnym	organizacyjne i techniczne	zabezpieczenie przed kodem złośliwym			
A10.5 Kopie zapasowe	organizacyjne i techniczne	próba odzyskania kopii			
A10.6 Zarządzanie bezpieczeństwem sieci	organizacyjne i techniczne	cechy bezpieczeństwa sieci			
A10.7 Obsługa nośników	organizacyjne i techniczne	zarządzanie nośnikami wymiennymi	bezpieczeństwo dokumentacji systemowej		
A10.8 Wymiana informacji	organizacyjne i techniczne	potwierdzenie elektronicznymi wiadomościami próbnymi zgodności z procedurami	transportowanie nośników fizycznych		
A10.9 Usługi handlu elektronicznego	organizacyjne i techniczne	autoryzacja dostępu		informacje dostępne publicznie	przeprowadzenie transakcji on-line
A10.10 Monitorowanie	organizacyjne i techniczne	rejestrowanie błędów		dzienniki audytu	monitorowanie użycia systemu
A11.1 Wymagania biznesowe wobec kontroli dostępu	organizacyjne i techniczne				
A11.2 Zarządzanie dostępem użytkowników	organizacyjne i techniczne	zarządzanie przywilejami			
A11.3 Odpowiedzialność użytkowników	organizacyjne	używanie haseł	polityka czystego biurka i ekranu		
A11.4 Kontrola dostępu do sieci	organizacyjne i techniczne	kontrola połączeń sieciowych			uwierzytelnianie użytkowników przy połączeniach zewnętrznych
A11.5 Kontrola dostępu do systemów operacyjnych	organizacyjne i techniczne	procedura bezpiecznego logowania się	zamykanie sesji po określonym czasie		testowanie czasu trwania połączenia

A11.6 Kontrola dostępu do aplikacji i informacji	organizacyjne i techniczne	ograniczenie dostępu do informacji			
A11.7 Przetwarzanie mobilne i praca na odległość	organizacyjne i techniczne				praca na odległość
A12.1 Wymagania bezpieczeństwa systemów informacyjnych	organizacyjne			zasady bezpieczeństwa	
A12.2 Poprawne przetwarzanie w aplikacjach	organizacyjne i techniczne	poprawność danych wejściowych i wyjściowych			
A12.3 Zabezpieczenia kryptograficzne	organizacyjne i techniczne	zarządzanie kluczami		polityka korzystania z zabezpieczeń krypto-graficznych	
A12.4 Bezpieczeństwo plików systemowych	organizacyjne i techniczne	kontrola dostępu do kodów źródłowych programów	ochrona systemowych danych testowych		
A12.5 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej	organizacyjne i techniczne	wyciek informacji		procedury kontroli zmian	
A12.6 Zarządzanie podatnościami technicznymi	organizacyjne i techniczne	rozprowadzanie poprawek technicznych			
A13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości	organizacyjne			zasady zgłaszania zdarzeń i słabości	
A13.2 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami	organizacyjne		zakresy odpowiedzialności		
A14.1 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania	organizacyjne	testowanie planów ciągłości działania	kontrola siedziby zapasowej		
A15.1 Zgodność z przepisami prawnymi	organizacyjne i techniczne	ochrona zapisów i danych osobowych			
A15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna	organizacyjne i techniczne	sprawdzenie zgodności technicznej			procesy dostępu i działania po sprawdzeniu
A15.3 Rozważania dotyczące auditu systemów informatycznych	organizacyjne i techniczne	ochrona narzędzi auditu			

Źródło: opracowanie własne na podstawie [8]

Skomplikowanym procesem wydaje się przeprowadzenie całego auditu ISMS z zastosowaniem wspomaganych komputerowo technik auditowania CAAT, jednocześnie dokument IAF MD 4:2008 precyzyjnie określa, iż działania z uwzględnieniem auditowania zdalnego CAAT nie powinny przekroczyć 30% czasu auditu założonego przez jednostkę certyfikującą dla danej organizacji [3]. Tak więc można, jak się wydaje, zastosować

technikę CAAT podczas auditu certyfikacyjnego, jak i auditów nadzoru jedynie w odniesieniu do badania niektórych z zabezpieczeń opisanych w tab. 2.

Jednostka certyfikująca podczas podejmowania decyzji o wykorzystywaniu CAAT podczas certyfikacji ISMS powinna uwzględnić następujące wymagania:

- poinformowanie jednostki akredytującej o stosowaniu CAAT,
- określenie zakresu auditu CAAT, czyli precyzyjne określenie kryteriów dla auditu CAAT, co w praktyce sprowadza się wskazaniem do testowania konkretnych zabezpieczeń ISMS oraz auditowania wybranych wymagań ISMS,
- określenie zakresu w jakim jednostka certyfikująca stosować będzie CAAT podczas oceny ISMS w odniesieniu do konkretnych branży,
- wybór technik do przeprowadzania zdalnego auditu CAAT,
- ustalenie zasad zapisywania wyników auditu oraz ich późniejszego archiwizowania.

3. Słabe i mocne strony stosowania wspomaganych komputerowo technik auditowania CAAT w certyfikacji ISMS

Zastosowanie wspomaganych komputerowo technik auditowania CAAT podczas przeprowadzania auditów ISMS wiąże się z zagrożeniami związanymi z prawidłowością, rozumianą jako zgodność z wymaganiami [6] i [8] oraz wiarygodnością przeprowadzonej oceny przez jednostkę certyfikującą. Dlatego istotne wydaje się oszacowanie ryzyka przez podstawowe zainteresowane strony, czyli jednostkę certyfikującą oraz certyfikowaną organizację. Przykładowe słabe i mocne strony zastosowania CAAT w certyfikacji ISMS zawarto w tab. 3.

Tab. 3. Słabe i mocne strony stosowania wspomaganych komputerowo technik auditowania CAAT.

	jednostka certyfikująca	**auditowania organizacja**
słabe strony	▪ konieczność oceny stopnia zrozumienia auditorów zasad CAAT, ▪ konieczność przechowywania zapisów elektronicznych z przeprowadzonych auditów CAAT, ▪ wdrożenie ISMS w jednostce certyfikującej, ▪ konieczność wyposażenia jednostki certyfikującej w odpowiedni sprzęt i oprogramowanie, ▪ ograniczenie związane z brakiem możliwości przemieszczania się po certyfikowanej organizacji, ▪ brak możliwości wykorzystanie tzw. tropów auditowych do prowadzenia auditu ISMS, polegających na badaniu kolejno procesów.	▪ konieczność udostępnienia dostępu do informacji dla auditorów ISMS, ▪ tzw. próba auditowa pobierana podczas auditu CAAT jest większa niż przy audicie klasycznym, co pociąga za sobą większe prawdopodobieństwo wychwycenia nieprawidłowości.
mocne strony	▪ wysokie kompetencje zespołu auditującego ISMS do	▪ wysokie kompetencje osób zarządzających w zakresie

	wykorzystania CAAT, ▪ skrócenie czasu auditu ISMS bezpośrednio w organizacji, ▪ liczne zapisy elektroniczne z przeprowadzonego auditu CAAT.	technik komputerowych wykorzystywanych podczas auditu, ▪ szybsze podejmowanie działań do uwag auditorów ISMS, ▪ krótszy czas auditu ISMS bezpośrednio w organizacji, ▪ przeprowadzenie oceny CAAT „z zewnątrz" wpływa na możliwość lepszej oceny zabezpieczeń.

Źródło: opracowanie własne

4. Podsumowanie i wnioski

Podsumowując należy stwierdzić, iż zastosowanie zasad wspomaganych komputerowo technik auditowania CAAT w auditowaniu systemu zarządzania bezpieczeństwem informacji ISMS powinno stać się praktyką stosowaną powszechnie przez jednostki certyfikujące. Przeprowadzanie auditu ISMS jest bezpośrednio powiązane z koniecznością przeprowadzenia testowania niektórych zabezpieczeń (tab.2) jeżeli zarówno jednostka certyfikująca, jak i certyfikowana organizacja uznają, że niektóre zabezpieczenia można testować zdalnie na odległość, to zastosowanie technik CAAT jest w tym przypadku niemal nieodzowne.

Kolejnym ważnym argumentem przemawiającym za stosowaniem technik CAAT w auditowaniu systemu zarządzania bezpieczeństwem informacji są wysokie kompetencje, zarówno zespołu auditującego ISMS, jak i osób odpowiedzialnych za funkcjonowanie ISMS w certyfikowanej organizacji, w zakresie wiedzy i umiejętności odnoszących się do stosowania w praktyce technik komputerowych. Jednocześnie zastosowanie komputerowo wspomaganych technik auditowania CAAT w praktyce nie jest związane z dodatkowymi kosztami ponoszonymi przez certyfikowaną organizację, ponieważ w większości jednostek certyfikujących koszt certyfikacji jest bezpośrednio powiązany z liczbą audito-dni. Koszty nie powinny bowiem ulec zmianie, ponieważ zmianie nie ulega czas trwania auditu systemu zarządzania bezpieczeństwem informacji, a jedynie następuje przesunięcie 30% czasu trwania auditu ISMS do auditu komputerowo wspomaganych technik auditowania CAAT. Zastosowanie wspomaganych komputerowo technik auditowania CAAT może znaleźć zastosowanie również podczas auditowania systemu zarządzania bezpieczeństwem informacji ISMS organizacji wieloodziałowej np. podczas auditowania systemu zarządzania bezpieczeństwem informacji ISMS w oddziałach i filiach banku [1].

W związku z dynamicznym rozwojem ilości certyfikacji w odniesieniu do systemu zarządzania bezpieczeństwem informacji ISMS, zarówno w Polsce, jak i na świecie, istotne staje się usprawnienie technik przeprowadzania auditów ISMS w certyfikowanych organizacjach. Jedną z najbardziej naturalnych oraz nowoczesnych technik przeprowadzania auditów wydaje się technika wspomagana komputerowo CAAT, tak spójna i zbieżna z zasadami stosowanymi w systemach zarządzania bezpieczeństwem informacji ISMS.

Literatura

1. IAF MD 1:2007; Dokument obowiązkowy International Accreditation Forum dotyczący zasad próbkowania w procesach certyfikacji organizacji wielooddziałowych.
2. IAF MD 3:2008; Dokument obowiązkowy International Accreditation Forum dotyczący zaawansowanych procedur nadzoru i ponownej certyfikacji.
3. IAF MD 4:2008; Dokument obowiązkowy International Accreditation Forum dotyczący stosowania wspomaganych komputerowo technik auditowania CAAT w akredytowanej certyfikacji systemów zarządzania.
4. IAF MD 5:2008; Dokument obowiązkowy International Accreditation Forum dotyczący ustalania czasu trwania auditów QMS i EMS.
5. PN-EN ISO 19011:2003 Wytyczne dotyczące auditowania systemów zarządzania jakością i/lub zarządzania środowiskowego.
6. PN-EN ISO/IEC 17021:2006 Ocena zgodności. Wymagania dla jednostek prowadzących auditowania i certyfikację systemów zarządzania.
7. PN-ISO/IEC 27001:2007 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania.
8. PN-ISO/IEC 27006:2009 Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji.
9. Polska Klasyfikacja Usług (PKD), Rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD), Dz.U. nr 251, poz. 1885.
10. Stoma M.: Rola pierwszego etapu auditu certyfikacyjnego w doskonaleniu systemu zarządzania środowiskiem opartym na wymaganiach normy PN-EN ISO 19011:2003, w: Wykorzystanie surowców rolniczych w energetyce, red. J.Tys, Wyd. Wieś Jutra, Warszawa 2009, s. 49-56.
11. Stoma M.: Ryzyko jednostki certyfikującej związane z niewłaściwą oceną wniosku o certyfikację systemów zarządzania, w: Zarządzanie jakością. Doskonalenie organizacji, red. T.Sikora, tom II, Wydawnictwo Naukowe PTTŻ, Kraków 2010, s. 224-234.
12. Stoma M., Dudziak A., Piekarski W., Zasady stosowania wspomaganych komputerowo technik auditowania CAAT (Komputer Assisted Auditing Techniques) w akredytowanej certyfikacji systemów zarządzania, [w:] Komputerowo zintegrowane zarządzanie, red. R.Knosala, tom II, Oficyna Wydawnicza PTZP, Opole 2011, s. 386 – 397.

Prof. dr hab. inż. Wiesław PIEKARSKI
Dr Monika STOMA
Mgr inż. Agnieszka DUDZIAK
Zakład Logistyki i Zarządzania Przedsiębiorstwem
Katedra Energetyki i Pojazdów
Wydział Inżynierii Produkcji
Uniwersytet Przyrodniczy w Lublinie
20-950 Lublin, ul. Akademicka 13
tel./fax.: (0-81) 531-83-15
e-mail: wieslaw.piekarski@up.lublin.pl
monika.stoma@up.lublin.pl
agnieszka.dudziak@up.lublin.pl