Programy audytów wybranych procesów/obszarów w zakładach ubezpieczeń cz. II

Podkomisja ds. Audytu i Kontroli Wewnętrznej
Komisji Ekonomiczno-Finansowej PIU
Warszawa, grudzień 2010 r.

PIU
Polska Izba Ubezpieczeń

SPIS TREŚCI

Szanowni Państwo,

Podkomisja ds. Audytu i Kontroli Wewnętrznej oddaje w Państwa ręce drugą część programów audytu wybranych procesów/obszarów funkcjonujących w zakładach ubezpieczeń. Część pierwsza (wydana w grudniu 2009 r.) zawierała programy audytu procesu naliczania i wypłaty prowizji agencyjnych, procesu likwidacji następstw zdarzeń objętych ochroną ubezpieczeniową, procesu reasekuracji oraz procesu zapewnienia ciągłości działania. Część druga zawiera programy audytu procesu tworzenia produktów, procesu ustalania i monitorowania składki, procesu sprzedaży, procesu zarządzania inwestycjami oraz program audytu bezpieczeństwa informacji, będący aktualizacją opracowania z 2005 r. (szczególnie o zapisy Polskiej Normy ISO/IEC 17799:2007).

Podobnie jak w części pierwszej, także w części drugiej każdemu obiektowi audytu (czyli podprocesowi lub podobszarowi danego procesu/obszaru poddawanego badaniu) przyporządkowana jest lista pytań, która powinna ułatwić badanie i ocenę adekwatności i efektywności systemu kontroli wewnętrznej i zarządzania ryzykiem w ramach każdego z nich. Listy pytań pomagają ponadto wyznaczyć kierunek prac, stanowią praktyczne podpowiedzi do planowania czynności audytowych, wykonania odpowiednich analiz i testów, zebrania niezbędnych dokumentów, danych i informacji, przeprowadzenia wywiadów i obserwacji.

Poszczególne listy pytań nie są kompletne – są jedynie wstępem do rozpoczęcia pracy nad właściwym programem audytu. Audytorzy przed rozpoczęciem zadania audytowego powinni bowiem dokładnie poznać i zrozumieć zasady funkcjonowania obszaru poddawanego badaniu, poznać główne procesy biznesowe, zidentyfikować potencjalne problemy i ryzyka biznesowe. Przeprowadzenie takiej analizy pozwoli na uzupełnienie każdego z prezentowanych w tym materiale programów o treści właściwe (i unikalne) dla procesu funkcjonującego w danym zakładzie ubezpieczeń.

Każdy z prezentowanych programów (list pytań) może być także uzupełniany w zależności od stopnia szczegółowości danego badania audytowego. Lista pytań do każdego z obiektów audytu danego procesu/obszaru może także stanowić zaczątek odrębnego i bardziej szczegółowego programu audytu, szczególnie wtedy, gdy przedmiotem audytu będzie tylko część danego procesu (np. bezpieczeństwo logiczne eksploatowanych systemów sieciowych i systemów informatycznych, planowanie sprzedaży, system monitorowania taryfikacji składki, monitorowanie produktu po jego wdrożeniu czy składanie zleceń i realizacja transakcji inwestycyjnych). Wybór zarówno zakresu, jak i sposobu wykorzystania należy do samych audytorów.

Tak jak w przypadku pierwszej części, mamy nadzieję, że materiał ten okaże się pomocny w usprawnieniu Państwa pracy i podwyższeniu profesjonalizmu podczas realizacji zadań audytowych.

PROGRAM AUDYTU PROCESU TWORZENIA PRODUKTU

Strategia i inne regulacje wewnętrzne związane z rozwojem produktów

1. Czy proces tworzenia i wyceny produktów realizuje zdefiniowane i zatwierdzone w zakładzie ubezpieczeń strategiczne cele biznesowe?
2. Czy została w zakładzie ubezpieczeń zdefiniowana polityka rozwoju produktów?
3. Czy procedura tworzenia i wyceny produktów została opracowana, formalnie zatwierdzona i jest stosowana? W szczególności, czy informacje dotyczące inicjatyw produktowych są odpowiednio chronione / zabezpieczone?
4. Czy w ramach procedury tworzenia i wyceny produktów (lub innym dokumencie) został ustalony jasny podział odpowiedzialności za kolejne fazy procesu? Czy ustalono także jasną odpowiedzialność za koordynowanie całego procesu?
5. Czy w ramach procedury tworzenia i wyceny produktów (lub innym dokumencie) jasno zdefiniowano kompetencje do zatwierdzania zakończenia kolejnych faz procesu oraz kluczowych dokumentów?
6. Czy w ramach procedury tworzenia i wyceny produktów (lub innym dokumencie) przygotowano, odpowiednio zatwierdzono oraz jest stosowana procedura tworzenia ogólnych warunków ubezpieczenia oraz innych dokumentów?
7. Czy w ramach procedury tworzenia i wyceny produktów (lub innym dokumencie) zostały zdefiniowane i są egzekwowane standardy jakości i wydajności tego procesu oraz czy określono drogę raportowania ich statusu w trakcie trwania procesu?
8. Czy zdefiniowano parametry i standardy pozwalające ocenić prawidłowość procesu tworzenia nowego produktu oraz wdrożenia do sprzedaży? Czy są one wykorzystywane przy każdym wdrożeniu?
9. Czy w zakładzie ubezpieczeń zdefiniowano i jasno zakomunikowano wszystkim w jaki sposób zbierane są pomysły dotyczące zmiany oferty produktowej czy też pomysły na nowe produkty?
10. Czy zakład ubezpieczeń zapewnia rozwój pracowników, aby utrzymać odpowiedni poziom kompetencji w procesie rozwoju i wyceny produktów? Czy zapewniono zastępowalność kluczowych kompetencji?

Analizy i analizowane dane

1. Czy prowadzone są bieżące analizy trendów rynku ubezpieczeń w zakresie oferty produktowej i serwisowej? Czy wyniki takich analiz są przekazywane do osób, które mają kompetencje podejmowania / inicjowania ewentualnych zmian w ofercie zakładu ubezpieczeń?
2. Czy na bieżąco monitorowane są i analizowane zmiany regulacji prawnych mających wpływ na kształt oferty produktowej?

3. Czy analizowane są na bieżąco potrzeby klientów oraz działalność konkurencji, a rezultaty tych analiz wykorzystywane są w procesie rozwoju produktów oraz tworzenia i wyceny nowych produktów?
4. Czy funkcjonuje proces identyfikacji potencjalnych szans pojawiających się na rynku w związku z działaniami konkurencji, zmianami przepisów prawa itd.? Czy zapewniony jest efektywny proces komunikowania takich szans i potencjał ich wykorzystania?
5. Czy na bieżąco wykonywane są wewnętrzne, kompleksowe analizy portfela produktów zakładu ubezpieczeń? W szczególności, czy na bieżąco oceniane jest czy oferowane przez zakład ubezpieczeń produkty nadal odpowiadają zakładanemu poziomowi jakości oraz zyskowności a także oczekiwaniom klientów (np. informacje z sieci sprzedaży, działu roszczeń / szkód, itd.)?
6. Czy skargi i reklamacje klientów oraz wszelkie komentarze związane z funkcjonowaniem portfela produktów zakładu ubezpieczeń są zbierane, rejestrowane, ocenione i wykorzystane do ustalania stopnia wymaganych zmian w ofercie zakładu ubezpieczeń?
7. Czy jest przeprowadzana pełna analiza kosztów procesu tworzenia i wyceny nowego produktu, a budżet jest formalnie zaplanowany i zapewniony?
8. Czy przeprowadzana jest analiza wpływu nowego produktu na istniejący portfel zakładu ubezpieczeń?

Proces tworzenia i wyceny nowego produktu / zmian produktów

1. Czy przy tworzeniu każdego z produktów analizowana jest jego zgodność ze strategicznymi celami biznesowymi zakładu ubezpieczeń?
2. Czy prowadzone s badania rynkowe a wyniki badań rynkowych są przekazywane odpowiednim osobom oraz analizowane przez kompetentne osoby? Czy decyzje podejmowane na podstawie danych z takich badań są właściwie dokumentowane?
3. Czy funkcjonują mechanizmy gwarantujące, że zostaną zapewnione właściwe środki i zasoby do stworzenia i wyceny nowego produktu zgodnie z przyjętymi założeniami i strategią? Czy ustalony jest budżet na rozwój produktu oraz dostępny jest odpowiednio wykwalifikowany personel?
4. Czy właściwie zaplanowane jest i zapewnione wsparcie pracowników lub podmiotów zewnętrznych posiadających odpowiednie kompetencje do przeprowadzania procesu tworzenia nowego produktu a w szczególności do jego wyceny?
5. Czy personel odpowiedzialny za tworzenie i wycenę nowego produktu ma odpowiednio zaplanowany i uzgodniony z przełożonymi podział zadań by zagwarantować terminowość prac związanych z nowym produktem?
6. Czy przebieg procesu tworzenia i wyceny nowych produktów jest analizowany pod kątem ryzyk i pojawiających się zagrożeń realizacji zaplanowanych działań? Czy wszelkie zagrożenia są ewidencjonowane, odpowiednio

przekazywane do osób, które mają kompetencje podejmowania decyzji, a problemy na czas rozwiązywane?

7. Czy kluczowe fazy procesu tworzenia i wyceny nowego produktu są odpowiednio kontrolowane? W szczególności, czy elementy manualne wyceny podlegają sprawdzeniu lub zatwierdzeniu?
8. Czy jest egzekwowany obowiązek zatwierdzania kluczowych kroków / dokumentów w procesie tworzenia nowego produktu? Czy uprawnienia odnośnie zatwierdzeń zostały odpowiednio nadane?
9. Czy jasno zostały zdefiniowane ryzyka ubezpieczeniowe nowego produktu? Czy zostały one właściwie udokumentowane i na czas przekazane osobom odpowiedzialnym za wycenę?
10. Czy dla opracowywanego produktu jest ustalony profil docelowego klienta / grupa docelowa?
11. Czy dokumentacja procesu wyceny jest kompletna i wystarczająca? Czy w sposób czytelny i kompletny dokumentowane są przyjęte założenia? Czy określono, jaka część założeń opiera się na analizie doświadczeń aktualnego portfela zakładu ubezpieczeń, jaka na analizie rynku a jaka jest przyjęta uznaniowo?
12. Czy zostało przeprowadzone niezależne sprawdzenie czy ustalony poziom składek jest wystarczający do pokrycia przyszłych zobowiązań / jest zgodny z ryzykami zdefiniowanymi dla produktu?
13. Czy dział prawny lub compliance na bieżąco / okresowo ocenia zgodność przyjmowanych i modyfikowanych założeń tworzonego produktu z obowiązującymi przepisami prawa oraz regulacjami wewnętrznymi zakładu ubezpieczeń?
14. Czy odpowiednio zaplanowane jest niezbędne wsparcie IT na etapie prowadzenia procesu tworzenia i wyceny nowego produktu jak również do obsługi powiększonego portfela zakładu ubezpieczeń? Czy niezbędne zmiany są wyceniane?
15. Czy zostały zdefiniowane wymagane zmiany w systemach IT niezbędne do obsługi nowego produktu zarówno na etapie sprzedaży jak i likwidacji szkód / obsługi świadczeń? Czy zostały one właściwie udokumentowane i na czas przekazane osobom odpowiedzialnym za wdrożenie?
16. Czy marketing został poinformowany o ostatecznym kształcie produktu by na czas przygotować strategie marketingową oraz wszelkie materiały marketingowe i informacyjne?
17. Czy niezbędne druki i formularze zostały zaprojektowane, przetestowane i zatwierdzone oraz na czas przekazane do publikacji?
18. Czy wnioski z analiz przeprowadzonych przed rozpoczęciem procesu tworzenia i wyceny nowego produktu zostały uwzględnione?
19. Czy możliwości dotyczące kanałów dystrybucji nowego produktu zostały przeanalizowane oraz udokumentowano decyzję wyboru określonych?
20. Czy zostały opracowane, przetestowane i sprawdzone procedury wewnętrzne niezbędne do sprawnego funkcjonowania i obsługi nowego produktu?

21. Czy zostały opracowane regulacje wewnętrzne zapewniające odpowiednie mechanizmy kontrolne na kluczowych etapach obsługi produktu po wdrożeniu?
22. Czy została przeanalizowana i potwierdzona zgodność nowego produktu i jego wyceny z planami sprzedażowymi?
23. Czy zostało odpowiednio zaplanowane ustanowienie kanałów przepływu informacji zwrotnej dotyczącej produktu i wykorzystania tej informacji?
24. Czy budżet czasu i środków przeznaczonych na tworzenie i wycenę nowego produktu był na bieżąco analizowany i realizowany?

Przygotowywanie wdrożenia i wdrażanie

1. Czy zostały zaplanowane i przeprowadzane kontrole zapewniające, że wszystkie istotne zagadnienia i ryzyka zostały uwzględnione i ocenione w procesie tworzenia nowego produktu oraz zaadresowane przed wdrożeniem produktu do sprzedaży?
2. Czy zostały na czas przygotowane i rozdystrybuowane właściwe materiały reklamowe i informacyjne, materiały szkoleniowe, formularze wewnętrzne i druki oraz instrukcje dla działów zaangażowanych w obsługę nowego produktu po jego wdrożeniu?
3. Czy zostało udokumentowane ostateczne potwierdzenie zgodności z prawem nowego produktu przed wdrożeniem do sprzedaży?
4. Czy struktury IT zostały przygotowane do wdrożenia i wyceny nowego produktu? Czy wprowadzone rozwiązania zostały przetestowane, a wszystkie błędy zostały usunięte przed rozpoczęciem sprzedaży?
5. Czy został przygotowany i przetestowany efektywny i sprawny obieg dokumentów i informacji? Czy wszystkie słabości zostały usunięte przed rozpoczęciem sprzedaży?
6. Czy zostało ocenione i potwierdzone przygotowanie odpowiednich struktur wewnętrznych zakładu ubezpieczeń do obsługi poszerzonej oferty produktowej?

Monitorowanie produktu po jego wdrożeniu

1. Czy w określonym czasie po wdrożeniu analizowana jest realizacja założeń ustalonych na etapie tworzenia i wyceny produktu? Czy wnioski z tych analiz zostały właściwie zaraportowane oraz wykorzystane?
2. Czy po wdrożeniu produktu oceniany jest poziom stosowania regulacji wewnętrznych zapewniających odpowiedni poziom efektywności mechanizmów kontrolnych i prawidłowości funkcjonowania produktu? Czy działania korygujące są na czas wdrażane?
3. Czy przeprowadzana jest analiza rzeczywistego funkcjonowania produktu na rynku po jego wdrożeniu? Czy

zdefiniowano jakie parametry podlegają analizie? Czy są ustalone standardy, w stosunku do których oceniany jest stopień spełnienia oczekiwań lub konieczność wprowadzania korekt do produktu?

W szczególności, czy analizowana jest:

- skuteczność underwritingu pozwalająca ocenić, czy wyłącznie wybrane i wycenione w procesie tworzenia produktu ryzyka są przez zakład ubezpieczeń przyjmowane do ochrony i na zakładanym poziomie;
- prawidłowość wyceny produktu pod względem jego rentowności, dopasowania do wyselekcjonowanych ryzyk oraz konkurencyjności na rynku?

4. Czy podczas analiz rzeczywistego funkcjonowania produktu na rynku po jego wdrożeniu pozyskiwane i wykorzystane są w szczególności informacje zwrotne z działów operacyjnych (np. informacje z sieci sprzedaży, działu roszczeń / szkód, itd.)?

PROGRAM AUDYTU PROCESU USTALANIA I MONITOROWANIA SKŁADKI

Regulacje wewnętrzne

1. Czy istniejące procedury zawierania umów ubezpieczeń obejmują wszystkie etapy procesu naliczenia składki ubezpieczeniowej (kwotowanie, ofertowanie, udzielania zniżek, zasady akceptacji i weryfikacji)?
2. Czy określono zasady udzielania zniżek? Czy procedury regulują limity dla poszczególnych szczebli struktury organizacyjnej?
3. Czy istnieją procedury określające zasady udzielania zgód na odstępstwa od obowiązujących taryf?

Taryfy

1. Czy istnieją mechanizmy zapewniające, że taryfy, które determinują wysokość składki były uprzednio autoryzowane i zaakceptowane?
2. Czy istnieją jasne zasady odpowiedzialności za system taryf?
3. Czy zostały określone zasady taryfikacji poszczególnych rodzajów umów dla danych grup produktowych?
4. Czy proces naliczania składki przebiega w sposób zautomatyzowany (z wykorzystaniem dedykowanych w tym celu narzędzi informatycznych – kalkulatorów), jednolity i przy zapewnieniu właściwego nadzoru?
5. Czy istnieją zasady aktualizacji taryf?

System monitorowania taryfikacji

1. Czy istnieją zasady doboru wskaźników w procesie monitorowania składki (np. składka przypisana, składka zarobiona, odnowienia, zwroty składek)?
2. Czy istnieje system monitorowania i raportowania dotyczący wysokości przypisu i inkasa w rozbiciu na poszczególne produkty ubezpieczeniowe? Czy uwzględnia występującą szkodowość?
3. Czy system zwyżek/zniżek jest analizowany pod kątem oceny zwiększonego ryzyka?
4. Czy dokonuje się analiz porównawczych danych o wysokości pobieranej składki z danymi uzyskanymi z niezależnych źródeł (np. dane rynkowe, prognozy)?
5. Czy przeprowadzany jest monitoring portfeli klientów? Jak wygląda proces takiego monitoringu Czy monitoring obejmuje dane dotyczące nowo pozyskanych i “utraconych” klientów?
6. Czy są monitorowane nietypowe transakcje (np. ze względu na sumę ubezpieczenia lub wysokość składki)?
7. Czy ustalono zasady częstotliwości płatności składki i czy jest nadzorowane ich przestrzeganie?
8. Czy procedury weryfikacji zawieranych umów ubezpieczeń obejmują weryfikację naliczonej składki ubezpieczeniowej?

Rozwiązania IT – wsparcie systemowe

1. Czy wszystkie istotne elementy systemów IT (kalkulatorów) wspierających proces naliczania składki były przedmiotem testów użytkowników końcowych lub innych niezależnych od wykonawcy systemu testów akceptacyjnych?
2. Czy system informatyczny (kalkulatory) umożliwia dostęp do wszystkich niezbędnych danych koniecznych do prawidłowego naliczania składki?
3. Czy funkcjonujące blokady systemowe uniemożliwiają wprowadzenie/modyfikowanie składek niezgodnych z taryfą?
4. Czy została opracowana procedura działania w sytuacji awaryjnej (niedostępności systemu informatycznego wspierającego proces naliczania składki)?

Szkolenia

1. Czy szkolenia produktowe dla pracowników akwizycji i współpracujących agentów obejmują również zagadnienia taryfikacji?

PROGRAM AUDYTU PROCESU SPRZEDAŻY

Strategia sprzedaży i regulacje wewnętrzne w obszarze sprzedaży

1. Czy zakład ubezpieczeń określił strategię sprzedaży? Czy jest udokumentowana i właściwie zaakceptowana i zakomunikowana?
2. Czy strategia sprzedaży jest spójna z celami strategicznymi zakładu ubezpieczeń? Dokonaj analizy zmian w strategii sprzedaży w porównaniu do poprzedniego okresu oraz oceń ich zakładany wpływ na wielkość, strukturę i dynamikę sprzedaży?
3. Czy założenia przyjęte do strategii nadal są aktualne? Jeśli uległy zmianie, czy strategia sprzedaży została zaktualizowana?
4. Czy w zakładzie ubezpieczeń zostały opracowane i wdrożone regulacje wewnętrzne w obszarze sprzedaży?
5. Czy regulacje wewnętrzne są aktualne i czy zostało wyeliminowane ryzyko sprzeczności z powszechnie obowiązującymi przepisami prawa?
6. Czy wbudowane w proces sprzedaży mechanizmy kontroli wewnętrznej są skuteczne (w tym, czy zapewniają przeciwdziałanie przestępczości ubezpieczeniowej i nadużyciom w strukturach sprzedaży)?
7. Czy w zakładzie ubezpieczeń funkcjonuje Kodeks Etyki? Czy jego postanowienia są komunikowane agentom? Czy w organizacji istnieje możliwość anonimowego zgłaszania zachowań nieetycznych (pracowników, agentów) ang. 'Whistleblower policy'?
8. Czy regulacje wewnętrzne dotyczące sprzedaży obowiązujące w zakładzie ubezpieczeń są dostępne dla wszystkich uczestników procesu sprzedaży, w tym pośredników ubezpieczeniowych?
9. Czy przebieg procesu sprzedaży w zakładzie ubezpieczeń został udokumentowany (formalnie opisany lub rozrysowany)? Czy zostały zidentyfikowane i ocenione ryzyka w tym procesie?
10. Czy istniejące procesy i procedury planowania sprzedaży są aktualne, zatwierdzone i zakomunikowane? Czy określono modele planowania wykorzystywane w procesie planowania sprzedaży (bottom up, top down, mieszane, format modelu sprzedaży)? Czy określono bazę do planowania sprzedaży (np. P/L, BSC, ABC, inne miary)? Jaka jest zasadnicza baza planowania sprzedaży (np. wynik w oparciu o rachunek zysków i strat, czy zrównoważona karta wyników, czy też rachunek kosztów działań)?
11. Czy określono właściciela i uczestników procesu planowania sprzedaży oraz ich funkcje i działania realizowane w tym procesie? Czy określono odpowiadzialnych za weryfikację danych wejściowych stanowiących podstawę do tworzenia planu?
12. Czy zakład ubezpieczeń określił zasady zarządzania i monitorowania sieci sprzedaży?

Planowanie sprzedaży (projekt, weryfikacja, wersja finalna planu sprzedaży)

Działania związane z przygotowaniem planów pożądanej wielkości, struktury i dynamiki sprzedaży produktow ubezpieczeniowych

PLANOWANIE

1. Czy zakład ubezpieczeń posiada opracowane regulacje, modele sprzedaży służące do przygotowania projektu planu sprzedaży? Czy proces jest uruchamiany w określonym terminie, kto jest inicjatorem? Kto jest ich właścicielem, kto odpowiada za akualizację i zgodność ze strategią (np. zmiany w kanałach dystrybucji, zmiany oferty produktowej)? W jaki sposób koordynowany jest proces z jednostkami terenowymi? Kto i w jaki sposób przekazuje i deleguje zadania w dół struktury sieci sprzedaży i ewentualnie zbiera informacje w drugą stronę?
2. Czy w procesie planowania sprzedaży uwzględniono model dystrybucji (np. sprzedaż wielokanałowa)? Czy w takiej sytuacji zakład uwzględnił wszelkie istotne różnice np. inne produkty, inne wsparcie, zasady współpracy, inne systemy motywacyjne itp.
3. Czy w przypadku modyfikacji planu sprzedaży weryfikowana jest spójność zmienionych planów sprzedażowych ze strategią zakładu ubezpieczeń? Czy propozycja zmiany planów sprzedażowych jest odpowiednio wcześnie komunikowana i konsultowana z akcjonariuszem i komórkami zaangażowanymi w jego realizację?
4. Czy w przypadku zmiany planów sprzedażowych przeanalizowano i udokumentowano następujące elementy:
   - obiektywne przesłanki zmiany planów;
   - racjonalne możliwości realizacji zmienionych planów;
   - poprawność realizacji zamierzeń;
   - formalny sposób zmiany.
5. Czy w zakładzie ubezpieczeń prowadzone jest regularne monitoriowanie rynku (badania rynku), w szczególności dotyczące trendów sprzedaży, jej dynamiki, możliwości wdrożenia nowych produktów (wynikających z regulacji prawnych i zmieniających się potrzeb klientów)? Czy proces monitorowania jest należycie udokumentowany?

WERYFIKACJA

1. Na jakim poziomie szczegółowości jest opracowany plan sprzedaży? Czy uwzględnia strukturę sieci sprzedaży (produkcja w wymiarze ilościowym i finansowym na poziomie agenta)?
2. Czy określono sposób wspierania jednostek terenowych w zakresie danych wejściowych (np. struktura sprzedawanych produktów, retencja agentów i ich produktywność itp.)? Czy istnieje niezależna weryfikacja, jeżeli jednostki terenowe samodzielnie przygotowują dane wejściowe?
3. Czy istnieją pisemne regulacje definiujące szczegółowość oraz sposób i terminy przygotowania ewentualnej propozycji do planu oraz ich weryfikacji w kolejnej fazie? Czy istnieje formalny proces negocjacji, uzgodnień w przypadku niezgodności? Czy określono kto podejmuje ostateczne decyzje? Czy sporządzany jest protokół

rozbieżności? Czy określono kto koordynuje zmiany w budżecie kosztów w związku z konsekwencjami zmian w planach sprzedaży (np. zwiększona rekrutacja, dodatkowe oddziały, więcej szkoleń w celu podniesienia jakości, koszty programów motywacyjnych i lojalnościowych)? Czy określono kto ostatecznie akceptuje opinie, uwagi i poprawki? Czy ostateczne decyzje są komunikowane czytelnie jednostkom terenowym?

PLAN FINALNY

1. Czy plan finalny jest efektem analizy relacji i zależności finansowych, aktuarialnych, operacyjnych, marketingowych, administracyjnych, informatycznych pod kątem realności i koordynacji?
2. Czy plan sprzedaży uwzględnia zaangażowanie agentów w obsługę 'starego portfela' i możliwości sprzedaży nowych produktów (możliwość rekomendacji i cross-selling)?
3. Czy przeprowadzono analizę wpływu wprowadzenia nowych produktów na istniejący portfel?
4. Czy zakład ubezpieczeń prowadzi i dokumentuje proces akceptacji planów sprzedaży na poszczególnych poziomach struktury organizacyjnej? Czy w przypadku zmian (rekrutacja nowych agentów, budowania nowych oddziałów, nowych struktur) proces ustalania celów sprzedażowych jest udokumentowany i skoordynowany z istniejącym i obowiązującym planem sprzedaży?
5. Czy proces planowania przebiegał zgodnie z procedurą, terminowo, z odpowiednim wsparciem itp.?

MONITOROWANIE PLANU

1. Czy realizacja planu sprzedaży jest monitorowana przez niezależne komórki, a wszelkie odchylenia wyjaśniane i raportowane do kierownictwa zakładu ubezpieczeń?
2. Czy zaprojektowano i wdrożono skuteczne mechanizmy kontrolne zapewniające, że dane stanowiące podstawę do rozliczeń planów sprzedaży są wiarygodne?

Rekrutacja i szkolenie agentów

Działania związane z budowaniem sieci sprzedaży opartej na agentach

1. Czy zakład ubezpieczeń opracował długoterminowy plan budowania sieci sprzedaży (rekrutacji agentów) zgodny ze strategią? Czy jest on zgodny z planem sprzedaży? Jakie główne mechanizmy zostały w tym planie uwzględnione? Czy mają one odpowiednie wsparcie w budżecie i w planach wszystkich uczestników procesu?
2. W przypadku gdy zakład ubezpieczeń nie ma opracowanego długoterminowego i szczegółowego planu rekrutacji agentów do sieci sprzedaży (np. manual procesu rekrutacyjnego, profil agenta itp) – jakie są sposoby i metody rekrutacji (np. każdy oddział, każda struktura realizuje proces indywidualnie)?
3. Czy określono kto i w jaki sposób przygotowuje i zatwierdza modele, programy i koszty rekrutacji?
4. Czy określono kto ostatecznie decyduje o podjęciu współpracy z kandydatem na agenta? Czy proces admini-

strowania agentami jest na tyle szczelny aby wychwycić osoby karane lub mające za sobą nieetyczną współpracę z innymi zakładami ubezpieczeń?

5. Czy analizowane są wskaźniki zrekrutowanych i przeszkolonych agentów do agentów aktywnych, z którymi podpisano umowę? Czy stosowane są mechanizmy zabezpieczające przed ponoszeniem zbędnych kosztów (np. czy zakład nie rekrutuje i szkoli dla innych?)
6. Czy w badanym okresie zidentyfikowano trendy w sieci sprzedaży (np. zwiększona fluktuacja)? Jeśli tak, z czego one wynikają? Czy i jakie ryzyko zidentyfikowano w związku ze stwierdzonymi trendami (np. ryzyko kluczowych sprzedawców i ryzyko kontrahenta)?
7. Czy agenci podlegają programowi ciągłego (ustawicznego) szkolenia w celu doskonalenia umiejętności sprzedaży?
8. Czy każdorazowo przed wdrożeniem nowych produktów na rynek zakład ubezpieczeń organizuje szkolenia dla agentów?
9. Czy zakład ubezpieczeń organizuje szkolenia obowiązkowe dla osób ubiegających się o wykonywanie czynności agencyjnych oraz dla osób wykonujących czynności agencyjne zgodnie z regulacjami zewnętrznymi (czy szkolenia organizowane przez zakład ubezpieczeń obejmują zakres zagadnień określonych w przepisach zewnętrznych, czy o terminie, miejscu szkolenia i egzaminu oraz składzie komisji egzaminacyjnej informowany jest organ nadzoru oraz czy powiadomienia te wysyłane są terminowo, czy występują przypadki przeprowadzania szkoleń obowiązkowych i egzaminów w jednostkach terenowych, do których agent został rekrutowany a nie w lokalizacjach zgłoszonych do organu nadzoru, jako miejsca odbycia szkolenia)?

Analiza potrzeb i oczekiwań klientów

Działania mające na celu pozyskanie nowych klientów oraz rozszerzenie współpracy z ubezpieczonymi w zakresie oferowanych przez zakład ubezpieczeń produktów ubezpieczeniowych.

1. Czy funkcjonuje baza danych klientów pozwalająca na ich jednoznaczną identyfikację?
2. Czy baza danych klientów pozwala na wskazanie produktów, które zakupił klient?
3. Czy baza danych klientów pozwala na identyfikowanie klientów w sposób dostarczający informacji o możliwości zaoferowania im innych produktów (np. adres, rodzina, nieruchomości, samochody, grupa zawodowa itp.)?
4. Czy prowadzone są badania potrzeb i oczekiwań klientów?
5. Czy prowadzone są analizy oferty produktowej pod kątem uwzględnienia oczekiwań klientów?
6. Czy zapewniono możliwość przekazywania przez klientów wniosków i opinii o produktach i działaniach sprzedawców?
7. Czy i w jaki sposób zbierane są i analizowane w zakładzie ubezpieczeń informacje na temat braku satysfakcji

Klientów z zakupionego produktu/ obsługi itp. (np.skargi)?

8. Czy zapewniono możliwość przekazywania przez klientów skarg i informacji o produktach i działaniach nieetycznych, niezgodnych z prawem?
9. Czy określono tryb i zasady postępowania (rozpatrywania) ze zgłoszonymi wnioskami, opiniami i skargami?
10. Czy zgłoszone wnioski, opinie i skargi są okresowo analizowane? Kto otrzymuje wyniki tych analiz?
11. Czy wyniki analiz są wykorzystywane w trakcie opracowywania produktów i doboru kanałów sprzedaży?
12. Czy określono zasady prowadzenia analiz preferencji klientów (częstotliwość, odbiorcy itp.)? Czy dotyczą one poszczególnych produktów oferowanych przez zakład ubezpieczeń, działań i produktów konkurencji itp.?
13. Czy w wyniku analiz preferencji klientów wdrożono nowe rozwiązania sprzedażowe? Czy dokonano analizy wpływu wdrożonych rozwiązań na rzeczywiście osiągane wyniki sprzedażowe?
14. Czy określono zasady prowadzenia analiz potrzeb klienta? Czy wyniki analiz są niezależnie weryfikowane (w stosunku do zaoferowanego produktu)?
15. Czy wyniki analizy potrzeb klienta uwzględniane są przy opracowywaniu nowych produktów?
16. Czy wyniki w/w analiz brane są pod uwagę przy wdrażaniu nowych produktów (np. czy przed wdrożeniem nowego produktu dokładnie testowane są możliwości obsługi danego produktu w całym cyklu życia produktu – od zawarcia umowy do wypłaty świadczenia)?

Akwizycja bezpośrednia

Działania mające na celu poinformowanie potencjalnych klientów o szczegółach oferowanych produktów ubezpieczeniowych

1. Czy opracowywane są materiały informacyjne i reklamowe dotyczące poszczególnych produktów? Czy treść tych materiałów jest rzetelna, zrozumiała i niewprowadzająca w błąd? Zweryfikuj, czy informacje kierowane do klientów:
   - nie ukrywają, nie umniejszają, nie przedstawiają w niejasny sposób istotnych elementów, stwierdzeń i ostrzeżeń,
   - przedstawiają w uczciwy, wyraźny i zrównoważony sposób potencjalne korzyści płynące z oferowanych produktów w zestawieniu z ewentualnymi wszelkimi powiązanymi zagrożeniami,
   - przedstawiają w uczciwy, wyraźny, miarodajny i zrównoważony sposób porównanie ubezpieczeniowych produktów inwestycyjnych, porównanie wyników osiągniętych w przeszłości i symulacje wyników w przyszłości, a także zawierają klauzule i ostrzeżenia wymagane przez powszechnie obowiązujące przepisy prawa i dobre praktyki rynkowe.
2. Czy określono zasady wizualizacji oraz wymogi co do eksponowania i dostępności materiałów informacyjnych

i reklamowych?

3. Czy zapewniono wsparcie informacyjne dla klientów ze strony zakładu ubezpieczeń (WWW, infolinia, callcenter, pośrednicy, pracownicy sprzedaży itp.)?
4. Czy określono zakres informacji i dokumentów wymaganych do uzyskania od klienta przy zawieraniu umowy i sposób ich potwierdzania?
5. Czy określono zakres informacji i dokumentów niezbędnych do przekazania (za potwierdzeniem) klientowi w trakcie zawierania umowy?

Techniki sprzedaży

1. Czy prowadzone są szkolenia sprzedawców/pośredników z zakresu technik sprzedaży?
2. Czy opracowywane (wdrażane) są narzędzia informatyczne wspomagające sprzedaż (automatyzujące pracę, ułatwiające wyliczenie składki, umożliwiające przeprowadzenie symulacji różnych wariantów ubezpieczenia)?

Przygotowanie i negocjowanie oferty oraz zawarcie umowy

1. Czy określono zakresy (limity) uprawnień dla sprzedawców do zawierania umów (suma ubezpieczenia, rodzaje produktów itp.)?
2. Czy określono zasady dokonywania oceny ryzyka ubezpieczeniowego i wyliczenia wysokości składki?
3. Czy określono zasady i kryteria stosowania zwyżek i zniżek?
4. Czy określono przypadki dopuszczalnych odstępstw od zasad ogólnych oceny ryzyka i określania wysokości składki?
5. Czy przypadki tych odstępstw są rejestrowane i okresowo weryfikowane?

Rozwój współpracy z klientami

1. Czy funkcjonują mechanizmy umożliwiające sprzedaż krzyżową i kojarzenie klientów i produktów?
2. Czy stosowane są mechanizmy rekomendacji pozwalające dotrzeć do innych klientów poprzez dotychczasowych klientów (przykładowo MGM – member get member)?
3. Czy prowadzony jest monitoring efektywności mechanizmów lojalnościowych (bonusy, zniżki marketingowe) pozwalających na utrzymanie i poszerzenie grupy klientów?

Jakość obsługi klienta

1. Czy określono wymagane standardy obsługi klientów i czy monitorowany jest sposób i tryb obsługi klientów?
2. Czy wyniki monitorowania i weryfikacji są wykorzystywane w trakcie opracowywania standardów sprzedaży

i doboru kanałów sprzedaży?

3. Czy określono zasady doboru i wymagania wobec sprzedawców?
4. Czy weryfikowane są okresowo kompetencje i umiejętności sprzedawców?

Opracowywanie, zamawianie i dystrybucja materiałów informacyjnych i reklamowych

1. Czy materiały informacyjno – reklamowe dotyczące produktów projektowane są na etapie opracowywania produktu i określania strategii sprzedaży?
2. Czy materiały informacyjno – reklamowe projektowane są w sposób uwzględniający strukturę sieci i potrzeby poszczególnych kanałów sprzedaży?
3. Czy jakość, forma i treść materiałów informacyjno – reklamowych dotyczących produktów jest opiniowana przez jednostki odpowiedzialne za produkty i sprzedaż?
4. Czy określono uprawnienia do zlecania wykonania materiałów informacyjnych i reklamowych i czy jest nadzorowane ich przestrzeganie?
5. Czy zapotrzebowanie na materiały informacyjno – reklamowe określane jest w powiązaniu z planami sprzedaży?
6. Czy nadzorowana jest zgodność formy i treści materiałów informacyjno – reklamowych z obowiązującymi zasadami wizualizacji (brandbook)?
7. Czy określono standardy jakościowe materiałów informacyjnych i reklamowych i czy jest nadzorowane ich stosowanie?
8. Czy materiały informacyjno-reklamowe zamawiane są przez jednostki organizacyjne racjonalnie tzn. w ilości/wartości proporcjonalnej do rozmiarów sieci sprzedaży i wielkości dotychczasowej/planowanej sprzedaży?
9. Czy określono zasady przydzielania jednostkom organizacyjnym materiałów informacyjno – reklamowych oraz ich wycofywania i czy jest nadzorowane przestrzeganie tych zasad?
10. Czy prowadzona jest ewidencja ilościowa/wartościowa rozdysponowanych materiałów informacyjno – reklamowych?
11. Czy zapewniono możliwość pilnego dostarczenia ponadplanowych ilości materiałów informacyjno – reklamowych?
12. Czy nadzorowana jest terminowość i kompletność dostaw zamówionych materiałów informacyjno – reklamowych?
13. Czy nadzorowane jest wypełnianie przepisów podatkowych (PIT8) związanych z rozdysponowaniem materiałów informacyjno – reklamowych?

Metody stymulowania wzrostu sprzedaży

Działania mające na celu określenie sposobów stymulowania wielkości sprzedaży

1. Czy przeprowadzono analizę zmian w założeniach systemu wynagrodzeń/ systemu prowizyjnego w ostatnim roku (okresie) oraz ich wpływu na wielkość sprzedaży?
2. Czy obecnie obowiązujący system wynagrodzeń sieci sprzedaży odpowiada / zapewnia realizację celów strategicznych Spółki?
3. Czy zakład ubezpieczeń okresowo analizuje efektywność zastosowanych metod stymulacji wzrostu sprzedaży (dochodowość inicjatyw w stosunku do nakładów poniesionych na te inicjatywy)?
4. Czy w zakładzie ubezpieczeń powołana została komórka organizacyjna, której zadaniem jest analiza trendów rynkowych oraz działań konkurencji – w celu doskonalenia oferty produktowej i usługowej zakładu ubezpieczeń?
5. Czy wyniki analiz przekazywane są na bieżąco i dyskutowane z osobami zarządzającymi siecią sprzedaży?

Metody mobilizowania sieci sprzedaży

Działania mające na celu określenie metod mobilizowania sieci sprzedaży do zwiększenia wielkości sprzedaży (konkursy; nagrody; wyższa prowizja).

1. Czy zakład ubezpieczeń opracował długoterminowy plan mobilizowania sieci sprzedaży ukierunkowany na wzrost wielkości sprzedaży (poza systemem wynagrodzeń/prowizyjnym)?
2. Jakie główne mechanizmy motywujące zostały w tym planie uwzględnione?
3. W przypadku gdy zakład ubezpieczeń nie ma opracowanego długoterminowego planu mobilizowania sieci sprzedaży (poza systemem wynagrodzeń/prowizyjnym) – jakie są najczęstsze przyczyny i okoliczności wdrażania inicjatyw motywujących sieć sprzedaży (np. wdrożenie nowego produktu, brak realizacji planów sprzedażowych pod koniec okresów raportowych, nasilenie działań konkurencji, czynniki lokalne itp)?
4. Czy określono zasady przygotowywania i zatwierdzania inicjatyw mających na celu mobilizację sieci sprzedaży do zwiększenia ilości sprzedaży (projekty, programy, pojedyncze inicjatywy)? Czy określono budżet, z którego finansowane są koszty prowadzenia tych inicjatyw (np. budżet departamentu sprzedaży, marketingu, inne zasoby)?
5. Czy określono zasady i kryteria prowadzenia konkursów i wyboru zwycięzców konkursów/ programów itp.? Jakie są to kryteria? Czy uwzględniają również jakość usług świadczonych przez agentów?
6. Czy przewidziane są mechanizmy działania w przypadku konfliktów/odwołań od wyników konkursów itp.? Na czym polegają te mechanizmy?
7. Czy po przeprowadzeniu konkursu weryfikowana jest jakość ‘produkcji’ zrealizowanej w ramach konkursu

(tj. czy konkursy, w których głównym kryterium jest sama sprzedaż produktu nie wpływają na znaczące obniżenie jakości usług świadczonych przez agentów)?

Analiza jakości sprzedaży i monitorowanie sprzedaży

1. Czy istnieją elementy zwiększające ryzyko przynoszenia ‘złej produkcji’ lub nadużyć (np. prowizja płatna z góry za rok, brak uzależnienia wynagrodzenia od jakości produkcji)?
2. Czy istnieją elementy kontroli jakości dot. produkcji (analiza lapsów i uzależnianie wynagrodzenia agentów od jakości sprzedaży)?
3. Czy funkcjonują mechanizmy kontroli zapewniające wykrywanie nadużyć (fałszerstwa, fikcyjne zawieranie umów, dla których w pierwszym okresie opłacana jest składka przez agenta – przez co otrzymuje on prowizję np. z góry za rok)?
4. Czy i w jaki sposób prowadzona jest analiza jakości sprzedaży i czy jej wyniki uwzględniane są w modelu wynagradzania agentów?
5. Czy dane wynikajace z analizy jakości sprzedaży są uzgadniane z danymi finansowymi?
6. Czy system analizy jakości sprzedaży uwzględnia analizę skarg dotyczących jakości sprzedaży obejmującą: źródła skarg, rodzaj zgłaszanych nieprawidłwości, przypadki nadużyć itp.?
7. Czy system analizy jakości sprzedaży uwzględnia wyniki analiz zewnętrznych (audyt zewnętrzny, audity jakości, audyt grupowy, badanie na zlecenie, kontrola zewnętrzna itp.)?

PROGRAM AUDYTU PROCESU ZARZĄDZANIA INWESTYCJAMI

Strategia i inne regulacje w obszarze inwestycji

1. Czy proces zarządzania inwestycjami realizuje zdefiniowane i zatwierdzone w zakładzie ubezpieczeń strategiczne cele biznesowe?
2. Czy strategia inwestycyjna została przyjęta przez właściwe organy zakładu ubezpieczeń?
3. Czy są inne regulacje wewnętrzne dotyczące zarządzania inwestycjami (np. dotyczące działania Komitetu Inwestycyjnego, zarządzania portfelami, limitów inwestycyjnych) i czy zostały przyjęte przez właściwe organy zakładu ubezpieczeń?
4. Czy obowiązujące procedury są kompletne? Czy precyzują sposoby zarządzania istotnymi ryzykami związanymi z działalnością inwestycyjną (tj. ryzykiem kredytowym, ryzykiem rynkowym, ryzykiem płynności i ryzykiem koncentracji?
5. Czy zostały wdrożone mechanizmy zapewniające, że strategia inwestycyjna i inne regulacje wewnętrzne są zgodne z obowiązującymi przepisami prawa?
6. Czy strategia i inne regulacje wewnętrzne zapewniają stały monitoring sytuacji finansowej partnerów inwestycyjnych (tj. emitentów, instytucji kredytowych, pożyczkobiorców)?
7. Czy strategia i inne regulacje wewnętrzne zapewniają dopasowanie aktywów i zobowiązań (terminy, waluty)?
8. Czy strategia i inne regulacje wewnętrzne zapewniają dywersyfikację przedmiotową i podmiotową inwestycji?
9. Czy strategia i inne regulacje wewnętrzne przewidują stosowanie mechanizmów zabezpieczających portfel inwestycji przed ryzykiem stopy procentowej?
10. Czy strategia i inne regulacje wewnętrzne zapewniają utrzymanie płynności? Czy została ustalona luka płynności, jeśli tak, czy jej poziom jest uzasadniony?

Realizacja stregii inwestycyjnej

1. Kto odpowiada za wykonanie strategii/ polityki inwestycyjnej?
2. Czy ustalone zostały jednoznaczne zakresy odpowiedzialności poszczególnych jednostek organizacyjnych oraz wybranych stanowisk w zakresie inwestycji?
3. Czy zostały powołane odpowiednie Komitety i czy ich skład jest prawidłowy (tj. czy uwzględnia udział osób o odpowiednim zakresie odpowiedzialności, czy w ich skład wchodzą również przedstawiciele reasekuracji i aktuariatu i zapewnia wyeliminowanie ryzyka konfliktu interesów)?
4. Czy ustalone zostały zasady współpracy, w tym przepływu informacji pomiędzy jednostkami organizacyjnymi oraz wybranymi stanowiskami w zakresie inwestycji?

5. Czy zarządzający posiadają pisemne pełnomocnictwa zawierające limity inwestycyjne? Czy ustalenie ww. limitów uwzględnia specyfikę portfeli tj. strukturę i skalę tych portfeli?
6. Czy konstrukcja systemu pełnomocnictw przewiduje przestrzeganie zasady kolektywności (np. przygotował, sprawdził, zatwierdził) w akceptacji decyzji inwestycyjnej?

Składanie zleceń i realizacja transakcji

1. W jaki sposób składane są zlecenia? Kto je akceptuje i w jakiej formie?
2. Czy złożone zlecenie jest dokumentowane (jaka jest jego forma materialna)? Gdzie i przez kogo jest przechowywana?
3. Jakiego rodzaju system wykorzystywany jest do składania zleceń? Czy dostępna jest aktualna dokumentacja użytkownika systemu?
4. Czy i w jaki sposób rejestrowane są zlecenia i transakcje?
5. Czy składanie zleceń jest nagrywane?
6. Kto i w jakim zakresie ma dostęp do systemu składania zleceń i rejestrowania transakcji?

Dokumentowanie, księgowanie składanych zleceń i transakcji

1. Czy decyzje transakcyjne są uzasadnione dokumentacją? Czy sposób jej przechowywania jest zgodny z przepisami prawa i regulacjami wewnętrznymi (w szczególności zapewnia weryfikację ex post prawidłowości podjętych decyzji inwestycyjnych?
2. Czy potwierdzenia zrealizowanych transakcji są przechowywane zgodnie z wymogami prawa i regulacjami wewnętrznymi?
3. Czy istnieje współpraca z zewnętrznymi firmami świadczącymi usługi finansowe w zakresie zarządzania aktywami? W jaki sposób dokonywany jest wybór w/w firm? Czy i z jaką częstotliwością prowadzona jest ich ocena? Czy zasady wynagradzania tych podmiotów motywują do zwiększania rentowności inwestycji przy akceptowalnym poziomie ryzyka?
4. Czy stworzona jest i na bieżąco aktualizowana lista inwestycyjna z limitami zaangażowania?
5. Czy proces zarządzania portfelami inwestycyjnymi jest prowadzony odrębnie od procesu wyceny i ewidencji księgowej inwestycji?
6. Czy współpraca pomiędzy zarządzającymi portfelami inwestycyjnymi a księgowością jest udokumentowana i zapewnia prawidłowe ujęcie inwestycji w księgach rachunkowych?
7. Jaki system wykorzystywany jest do prowadzenia wyceny i ewidencji inwestycji? Czy dostępna jest aktualna dokumentacja użytkownika dla tego systemu?

8. Kto i w jakim zakresie ma dostęp do systemu wyceny i ewidencji inwestycji?
9. Czy, w jakim celu i z jaką częstotliwością są wykonywane wydruki z systemu?

Nadzór nad przebiegiem procesu inwestycyjnego

1. Czy i w jaki sposób zorganizowany jest nadzór nad przebiegiem procesu inwestycyjnego?
2. Czy i w jaki sposób wykonywany jest nadzór nad przestrzeganiem udzielonych pełnomocnictw (kompetencji, uprawnień, limitów inwestycyjnych)?
3. Czy i jakie mierniki stosowane są do oceny efektywności zarządzania?
4. Czy adekwatność modeli finansowych (jeśli są stosowane) wykorzystywanych do działalności inwestycyjnej jest okresowo badana?

Konflikt interesów

1. Czy wprowadzone zostały regulacje dotyczące konfliktu interesów w przypadku pracowników mających dostęp do informacji o działalności inwestycyjnej zakładu?
2. Czy regulacje dotyczące konfliktu interesów zawierają zasady dotyczące inwestycji pracowników na rachunek własny, osób trzecich (w tym osób fizycznych, jak i podmiotów, za pośrednictwem których pracownicy lub osoby im bliskie i spokrewnione z nimi mogą osiągać korzyści majątkowe), zasady w zakresie przyjmowania prezentów i innych korzyści oraz zasady raportowania?
3. Czy, w jaki sposób i z jaką częstotliwością dokonywana jest kontrola przestrzegania tych zasad?

Statystyka, raportowanie

1. Czy zostały zdefiniowane raporty (obligatoryjne, nieobligatoryjne, wewnętrzne, zewnętrzne) i kto jest ich adresatem (np. organy zakładu, udziałowcy, podmioty współpracujące, instytucje nadzorcze) i z jaką częstotliwością są sporządzane i przekazywane?
2. Czy wyznaczone zostały osoby do wykonywania i autoryzacji raportów?
3. Czy, w jaki sposób i z jaką częstotliwością przeprowadzana jest analiza wskaźnikowa w zakresie inwestycji (wskaźniki rentowności oraz inne w odpowiednich konfiguracjach)?
4. Czy istnieją definicje, wzory, wyznaczone dopuszczalne wartości min i max wskaźników?
5. Czy raporty generowane są automatycznie z systemów informatycznych i czy możliwa jest oraz w jakim zakresie ich modyfikacja?
6. Czy, przez kogo i z jaką częstotliwością sporządzane są sprawozdania dotyczące zarządzanych portfeli?

Współpraca z podmiotami zewnętrznymi

1. Czy w zakładzie ubezpieczeń przyjęte zostały i są stosowane kryteria wyboru podmiotów zewnętrznych do współpracy w procesie inwestycji?
2. Jakie zostały zastosowane zasady wyboru ww. podmiotów? W jakim horyzoncie czasowym następuje weryfikacja listy podmiotów współpracujących?
3. Czy z podmiotami zewnętrznymi zostały podpisane umowy o współpracy?
4. Czy warunki zawartych umów zabezpieczają interesy zakładu ubezpieczeń?
5. Czy, w jaki sposób i z jaką częstotliwością kontrolowana jest jakość czynności wykonywanych przez podmioty zewnętrzne oraz ich zgodność z ustalonymi wymaganiami?
6. Czy i z jaką częstotliwością analizowana jest efektywność współpracy z podmiotami zewnętrznymi?
7. Czy są określone i przestrzegane konsekwencje wynikające z ewentualnego niewywiązywania się z warunków współpracy przez podmiot zewnętrzny?
8. Czy, w jaki sposób i z jaką częstotliwością kontrolowana jest prawidłowość rozliczeń z podmiotami zewnętrznymi?
9. Czy istnieje współpraca z zewnętrznymi firmami świadczącymi usługi finansowe w zakresie zarządzania aktywami? W jaki sposób dokonywany jest wybór w/w firm? Czy i z jaką częstotliwością prowadzona jest ich ocena? Czy zasady wynagradzania tych podmiotów motywują do zwiększania rentowności inwestycji przy akceptowalnym poziomie ryzyka?

Funkcjonalność systemu informatycznego wspierającego proces inwestowania

1. Czy proces inwestycyjny przebiega z wykorzystaniem dedykowanego w tym celu narzędzia informatycznego (systemu)? Czy do wszystkich rodzajów inwestycji danego zakładu ubezpieczeń zostały dedykowane odpowiednie narzędzia informatyczne?
2. Czy jest to system umożliwiający dostęp do odpowiednich danych wszystkim komórkom wewnętrznym zaangażowanym w proces inwestycji lub wykorzystujących dane o inwestycjach w ramach swoich procesów?
3. Czy funkcjonalność systemu umożliwia odtworzenie wszystkich etapów procesu inwestycji?
4. Czy funkcjonalność systemu umożliwia uwzględnienie dodatkowych informacji istotnych z punktu widzenia procesu inwestycji?
5. Czy w procesie inwestycji wykorzystywane są specjalistyczne programy informatyczne identyfikujące nieprawidłowości w procesie inwestycji (np. niedopasowanie inwestycji i zobowiązań pod względem terminów, walut, przekroczenie limitów ustawowych pod względem koncentracji przedmiotowej i podmiotowej, wewnętrznych limitów decyzyjnych, uprawnień, potencjalnego konflikt interesów)?
6. Czy została opracowana procedura działania w sytuacji awaryjnej (np. awaria sieci komputerowej)?

PROGRAM AUDYTU PROCESU BEZPIECZEŃSTWA INFORMACJI

Wprowadzenie

W kwietniu 2005 roku Grupa Robocza ds. Audytu i Kontroli Wewnętrznej w ramach Komisji Ekonomiczno-Finansowej Polskiej Izby Ubezpieczeń opracowała i opublikowała dokument „Audyt bezpieczeństwa informacji – rekomendacje". Opracowanie to wychodziło naprzeciw oczekiwaniom audytorów wewnętrznych w zakładach ubezpieczeń w zakresie zagadnień istotnych przy wykonywaniu audytów bezpieczeństwa informacji. Niniejszy dokument jest aktualizacją opracowania z 2005 roku. Zmiany objęły w szczególności:

- Uzupełnienie wszystkich rozdziałów zgodnie z zapisami Polskiej Normy ISO/IEC 17799:2007 oraz kolejnymi pięcioma latami doświadczenia tworzących opracowanie.
- Usunięcie z dokumentu rozdziału poświeconego planowaniu awaryjnemu, zapewniającego „ciągłość działalności", gdyż temat ten został już po kwietniu 2005 roku objęty dedykowanym opracowaniem (patrz: „Programy audytów wybranych procesów/obszarów w zakładach ubezpieczeń, cz. I") .
- Dodanie rozdziału „Zgodność z przepisami obowiązującego prawa"

Ogólne zagadnienia dotyczące audytu bezpieczeństwo informacji

Szybkość zmian dokonujących się w świecie biznesu i dynamika rozwoju cywilizacyjnego doprowadziły do sytuacji, że coraz częściej wdrożenie i utrzymanie systemu bezpieczeństwa informacji jest dla współczesnego przedsiębiorstwa niezbędnym warunkiem jego bezpiecznego funkcjonowania na rynku. Brak odpowiedniego zabezpieczenia informacji może stanowić o losach całej organizacji, jej funkcjonowaniu i wiarygodności.

Informacja może być zapisana na papierze, może być przechowywana w formie elektronicznej. Może być przesyłana pocztą tradycyjną lub przy pomocy urządzeń elektronicznych. Może też być przekazana w formie tradycyjnej – w trakcie rozmowy. Niezależnie od tego, w jakiej formie występuje informacja i jak jest przekazywana, ma zawsze takie samo znaczenie dla przedsiębiorstwa i powinna być w odpowiedni sposób chroniona.

Dla celów dalszych analiz istotne jest określenie definicji pojęć dane i informacje. Przy tworzeniu niniejszego opracowania przyjęte zostało, iż jako dane rozumiemy każdy rodzaj zapisu znaków zarówno w formie elektronicznej jak i papierowej, którego interpretacja nie jest możliwa bez dodatkowych narzędzi lub specjalistycznej wiedzy. Jako informacje rozumiane są dane przetworzone w ten sposób, iż ich interpretacja możliwa jest dla zainteresowanych osób posiadających rozsądny (reasonable) poziom wiedzy w danym zakresie. W świetle tej definicji można przytoczyć przykład, iż zapisy sald na kontach, czyli tzw. obrotówka to dane, a opracowane na tej podstawie sprawozdanie finansowe to informacja. Pomimo, iż zaproponowane definicje mają charakter subiektywny i uzależniają podział na dane i informacje od poziomu wiedzy odbiorcy, umożliwiają systematyzację podejścia do dalszej analizy bezpie-

czeństwa informacji. Bezpieczeństwo informacji jest rozumiane jako zachowanie jej trzech cech:

1. poufności – tzn. zapewnienie dostępu do informacji tylko osobom autoryzowanym
2. integralności – tzn. zabezpieczenie dokładności i kompletności informacji oraz metod jej przetwarzania
3. dostępności – tzn. zapewnienie autoryzowanym użytkownikom dostępu do informacji

Analizując problem bezpieczeństwa należy brać pod uwagę zagrożenia, jakie może przynieść nieodpowiednie postępowanie z informacjami. W przypadkach szczególnych zakład ubezpieczeń może być narażony na straty materialne, które mogą być spowodowane np. wyciekiem informacji i/lub danych lub podjęciem, na podstawie nieprawdziwych lub niepełnych danych bądź informacji – błędnych decyzji. Pamiętać też należy o odpowiedzialności karnej i cywilnej, którą nakładają regulacje ogólne, za nieodpowiednie zabezpieczenie pewnych informacji (np. dane osobowe).

Bezpieczeństwo jest narażone na zagrożenia wewnętrzne i zewnętrzne. Mogą to być świadome działania wymierzone przeciwko naszemu przedsiębiorstwu. Częściej będą to problemy infrastruktury technicznej lub działania czynników środowiskowych. Jednak najczęściej będzie to nieodpowiednie działanie własnych pracowników. W wielu wypadkach będzie to niezamierzone działanie wynikające z nieświadomości zagrożeń, na jakie może być narażone przedsiębiorstwo w wyniku nieodpowiedniego postępowania z informacją.

Rozwijając tą myśl można pokusić się o stwierdzenie, że aby określić, czy informacje chronione są w sposób zabezpieczający żywotne interesy zakładu ubezpieczeń wystarczy sprawdzić, czy pracownicy wiedzą, które informacje powinny być chronione. Niestety nie jest to takie proste. Sama świadomość pracowników nie wystarczy. Bez wdrożenia odpowiedniego i co najważniejsze sprawnie działającego systemu bezpieczeństwa informacji, nasz zakład ubezpieczeń może być narażony na różnego rodzaju niebezpieczeństwa.

Załączony wykaz pytań umożliwia ogólną ocenę systemu kontroli bezpieczeństwa informacji w naszym zakładzie ubezpieczeń. Zakres obszarów oparty jest na ogólnie przyjętych standardach w tym Polskiej Normie ISO/IEC 17799:2007 oraz własnych doświadczeniach.

Uzyskana ocena będzie stanowić punkt wyjścia do głębszej analizy potrzeby usprawnienia systemu kontroli. Jednocześnie jej wyniki pozwolą na określenie obszarów, jakie powinny zostać poddane audytowi informatycznemu. Audyt informatyczny powinien być oparty na specjalistycznych narzędziach, jakim jest np. istniejący standard audytu środowiska informatycznego – COBIT (Control Objectives For Information and Related Technology) lub wspominana wcześniej Polska Norma ISO/IEC 17799:2007. Pamiętajmy jednak, że gdy będziemy chcieli przeprowadzić audyt wymagający specjalistycznej wiedzy (np. testy penetracyjne naszych systemów informatycznych) najlepszym rozwiązaniem będzie zaangażowanie do tego zadania odpowiednich specjalistów.

Bezpieczeństwo informacji jest przedmiotem szeregu regulacji zewnętrznych. W związku z tym istotne jest, aby w trakcie audytu zidentyfikować, które z regulacji zewnętrznych dotyczą audytowanych działalności zakładu

ubezpieczeniowego. Po dokonaniu identyfikacji regulacji zewnętrznych wymagane jest uzupełnienie wybranych zagadnień opisanych w kolejnej części dokumentu o dodatkowe zagadnienia wynikające specyficznie ze zidentyfikowanych regulacji. Regulacjami związanymi z bezpieczeństwem informacji, które dotyczą każdego zakładu ubezpieczeniowego są:

- Ustawa o działalności ubezpieczeniowej.
- Ustawa o ochronie danych osobowych.
- Kodeks spółek handlowych.
- Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Pozostałe regulacje związane z bezpieczeństwem informacji mogące dotyczyć zakładów ubezpieczeń to m.in.:

- Ustawa o świadczeniu usług drogą elektroniczną.
- Ustawa o podpisie elektronicznym.
- Dyrektywa Solvency II.
- Kodeks pracy

Dla podkreślenia znaczenia systemu bezpieczeństwa informacji poniżej cytowany jest Art. 52 Ustawy o ochronie danych osobowych (Dz. U. 101 z 2002 r., poz. 926, z późniejszymi zmianami), który nie powinien pozostawić żadnych wątpliwości, gdy zada się pytanie : *Chronić nasze dane czy nie?* W tym przypadku dane osobowe. A z takimi danymi jako zakłady ubezpieczeń mamy najczęściej do czynienia.

„Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.”

Analiza ryzyka

1. Czy zakład ubezpieczeń dokonał wyjściowej analizy istotności ryzyk związanych z naruszeniem bezpieczeństwa informacji?
2. Czy analiza istotności ryzyk związanych z naruszeniem bezpieczeństwa informacji jest cyklicznie aktualizowana?
3. Czy określone zostały zasady postępowania z ryzykami w zakresie bezpieczeństwa informacji? Może to mieć miejsce w ogólnej polityce zarządzania ryzykiem w zakładzie ubezpieczeń lub też w dokumencie dedykowanym obszarowi bezpieczeństwa informacji.

Polityka bezpieczeństwa informacji

1. Czy Zarząd zakładu ubezpieczeń wyodrębnił ze swego grona lub wskazał osoby odpowiedzialne za wyraźne określanie polityki w dziedzinie bezpieczeństwa informacji?
2. Czy w zakładzie ubezpieczeń dokonana została analiza kosztów jakie należałoby ponieść na zabezpieczenie informacji w odniesieniu do strat, na jakie mógłby z tego tytułu być narażony zakład ubezpieczeń?
3. Czy wykonywane są, przez Zarząd zakładu ubezpieczeń lub przez osoby wskazane, przeglądy naruszeń bezpieczeństwa informacji?
4. Czy w zakładzie ubezpieczeń opracowana i wdrożona została polityka bezpieczeństwa informacji?
5. Czy polityka bezpieczeństwa informacji jest przedmiotem cyklicznej weryfikacji i aktualizacji?
6. Czy w zakładzie ubezpieczeń funkcjonują regulacje szczegółowe, dotyczące poszczególnych systemów informatycznych lub określające zasady bezpieczeństwa przy obchodzeniu się z danymi i informacjami?
7. Czy w zakładzie ubezpieczeń jest prowadzony rejestr naruszeń bezpieczeństwa informacji (incydentów)?

Organizacja bezpieczeństwa informacji

1. Czy ustalone zostały jednoznaczne zakresy odpowiedzialności poszczególnych jednostek organizacyjnych oraz wybranych stanowisk w zakresie kontroli bezpieczeństwa informacji?
2. Czy w zakładzie ubezpieczeń powołana została wyodrębniona funkcja odpowiedzialna za koordynację kontroli bezpieczeństwa informacji?
3. Czy ustalone zostały zasady współpracy, w tym przepływu informacji pomiędzy jednostkami organizacyjnymi oraz wybranymi stanowiskami w zakresie kontroli bezpieczeństwa informacji?
4. Czy ustalone są sposoby kontaktowania się z organami ścigania, organami wydającymi przepisy, dostawcami usług informatycznych oraz telekomunikacyjnych, w celu szybkiego uruchomienia stosownych działań i pomocy w przypadku naruszenia bezpieczeństwa?
5. Czy w zakładzie ubezpieczeń są zidentyfikowane osoby (posiadające z reguły szeroki dostęp do informacji), któ-

re mogą być celem ataku polegającego na wymuszeniu dostępu? Jeżeli tak to czy ustalone są „alarmy przymusu" i sposoby reagowania na takie alarmy?

6. Czy nowe lub zmodyfikowane systemy informatyczne są weryfikowane przed wdrożeniem w zakresie organizacji bezpieczeństwa informacji w tych systemach i dopuszczane do eksploatacji po przejściu pozytywnej weryfikacji?
7. Czy nowe lub zmodernizowane powierzchnie biurowe wraz z wyposażeniem są weryfikowane w kontekście możliwości zapewnienia bezpieczeństwa przetwarzanych w tych pomieszczeniach informacji, czy wnioski z weryfikacji są wcielane w życie?
8. Czy możliwe jest użytkowanie urządzeń nie będących własnością zakładu ubezpieczeń do przetwarzania informacji związanych z działalnością zakładu ubezpieczeń?
9. Czy przy przetwarzaniu informacji zakład ubezpieczeń korzysta z usług zewnętrznych organizacji, jeżeli tak to, czy umowy z dostawcami tych usług oraz stosowane przez tych dostawców mechanizmy kontrolne gwarantują odpowiednie warunki bezpieczeństwa?
10. Czy występują sytuacje (np. współpraca lub naprawa sprzętu), w których zakład ubezpieczeń udziela podmiotom zewnętrznym, dostępu do własnych systemów informatycznych lub do urządzeń zawierających dane/informacje?
11. Czy zakład ubezpieczeń korzysta w swojej siedzibie z usług podmiotów zewnętrznych (np. serwis techniczny, sprzątanie) i czy w związku z tym określone są warunki bezpieczeństwa, jakie powinny być zachowane w stosunku do infrastruktury, w której przechowywane są dane/informacje (np. komputery, szafy z aktami)?
12. Czy zakład ubezpieczeń posiada wzory umów o zachowaniu poufności w sytuacji współpracy z podmiotami zewnętrznymi?
13. Czy wzory umów o zachowaniu poufności są przedmiotem cyklicznych przeglądów?
14. Czy zakład ubezpieczeń posiada zasady zabezpieczania informacji w kontaktach z klientami?

Zasady klasyfikacji zasobów informacyjnych

1. Czy w zakładzie ubezpieczeń zdefiniowane są indywidualne zasoby informacyjne (pojedyncza informacja lub zbiór informacji dotyczących tego samego zagadnienia)?
2. Czy są wskazane, w sposób formalny, osoby odpowiedzialne za każdy z zasobów informacyjnych?
3. Czy są zdefiniowane i w formalny sposób zatwierdzone poziomy uprawnień do poszczególnych zasobów informacyjnych?
4. Czy zidentyfikowane zostały rodzaje danych lub informacji, co do ich ważności, obejmujące w szczególności informacje lub dane wrażliwe, do których dostęp powinien być ograniczony?
5. Czy informacje i dane wyjściowe uzyskiwane zarówno z dokumentacji papierowej jak i z systemów infor-

matycznych mają zdefiniowany i znany pracownikom, stopień ważności dla zakładu ubezpieczeń oraz czas, po którym przestają mieć znaczenie?

Bezpieczeństwo związane z personelem

1. Czy obowiązki pracowników w zakresie zachowania bezpieczeństwa informacji są uwzględnione w umowie o pracę/regulaminie pracy?
2. Czy pracownicy zakładu ubezpieczeń, gdy są przyjmowani do pracy lub zmieniają stanowisko, są szkoleni z zakresu bezpieczeństwa informacji?
3. Czy wszyscy pracownicy i podmioty zewnętrzne poinformowani zostali w sposób formalny o obowiązku zgłaszania wszelkich naruszeń systemów (np. złamanie zabezpieczeń, niewłaściwa praca, wolniejsza praca)?
4. Czy istnieją zasady informowania przełożonych o zidentyfikowanych sytuacjach narażających zakład ubezpieczeń na utratę bezpieczeństwa informacji?
5. Czy w zakładzie ubezpieczeń prowadzone są formalne postępowania dyscyplinarne w stosunku do pracowników naruszających zasady bezpieczeństwa lub przyczyniających się do stworzenia zagrożenia dla bezpieczeństwa informacji?
6. Czy wszyscy pracownicy posiadają wyznaczone strefy dostępu fizycznego?

Bezpieczeństwo fizyczne i środowiskowe

(**dotyczy także pomieszczeń, w których przechowywana jest dokumentacja papierowa, zawierająca informacje chronione**).

1. Czy urządzenia komputerowe służące do przechowywania i przetwarzania danych i informacji wrażliwych dla zakładu ubezpieczeń, znajdują się w pomieszczeniach bezpiecznych (z punktu widzenia analizy ryzyka np. nie są usytuowane na parterze, nie grozi im zalanie, okna są zabezpieczone i zasłonięte, w pobliżu nie ma materiałów łatwopalnych)?
2. Czy wrażliwa dokumentacja papierowa przechowywana jest w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieuprawnionych oraz działaniem czynników środowiskowych?
3. Czy pomieszczenia zakładu ubezpieczeń, ze szczególnym uwzględnieniem miejsca przetwarzania wrażliwych danych i informacji, są wyposażone w automatyczne systemy przeciwpożarowe?
4. Czy oznaczenie budynków lub obszarów, w których znajdują się urządzenia zawierające wrażliwe dane i informacje lub kluczowe składniki systemu informatycznego (serwerownie, węzły sieci logicznej), sugerują znajdującą się tam zawartość?
5. Czy w wewnętrznych spisach telefonów, dokumentach ogólnie dostępnych lub w oficjalnych publikacjach są za-

warte informacje pozwalające zidentyfikować pomieszczenia służące do przechowywania i przetwarzania danych i informacji wrażliwych dla zakładu ubezpieczeń?

6. Czy urządzenia komputerowe i inne urządzenia służące do przechowywania wrażliwych danych i informacji usytuowane są w pomieszczeniach do, których dostęp mogą mieć tylko osoby uprawnione?
7. Czy na terenie obszarów, w których znajdują się pomieszczenia z urządzeniami zawierającymi informacje wrażliwe dane i informacje, osoby tam przebywające mają obowiązek noszenia identyfikatorów?
8. Czy goście z zewnątrz przez cały czas swojego pobytu, na terenie obszarów, w których znajdują się pomieszczenia z urządzeniami zawierającymi wrażliwe dane i informacje, przebywają w towarzystwie pracownika ochrony lub wyznaczonego pracownika merytorycznego?
9. Czy w zakładzie ubezpieczeń wprowadzone zostały w sposób formalny zasady przewożenia i korzystania z przenośnego sprzętu komputerowego w miejscach publicznych (np. zakaz pozostawiania sprzętu bez nadzoru w miejscach publicznych, nakaz przewożenia komputerów przenośnych w taki sposób, aby osoby postronne nie wiedziały o jego istnieniu)?
10. Czy w zakładzie ubezpieczeń obowiązuje zasada „czystego biurka i czystego ekranu", tzn. czy po zakończeniu pracy lub przy wyjściu z pokoju cała dokumentacja jest w odpowiedni sposób zabezpieczona lub schowana a komputer wyłączony lub zablokowany hasłem?
11. Czy prowadzona jest ewidencja wynoszonego poza siedzibę sprzętu, oprogramowania, danych lub informacji?

Zarządzanie systemami sieciowymi, systemami informatycznymi i sprzętem teleinformatycznym

1. Czy zakład ubezpieczeń jest w posiadaniu aktualnej dokumentacji swoich systemów komputerowych?
2. Czy prowadzony jest spis wszystkich urządzeń komputerowych wykorzystywanych w zakładzie ubezpieczeń, wraz ze wskazaniem miejsca instalacji lub użytkownika?
3. Czy w zakładzie ubezpieczeń prowadzony jest spis wszystkich programów i aplikacji dopuszczonych do użytkowania w systemach informatycznych wraz ze wskazaniem miejsca zainstalowania?
4. Czy w urządzeniach komputerowych lub w systemach informatycznych służących do przechowywania i przetwarzania danych i informacji zmian dokonywać mogą tylko osoby do tego upoważnione?
5. Czy wszystkie zmiany dokonane w urządzeniach komputerowych i systemach informatycznych są ewidencjonowane w sposób umożliwiający ustalenie m.in. zatwierdzającego dokonanie zamian, ich celu i zakresu?
6. Czy zastosowane rozwiązania informatyczne zapewniają synchronizację czasu w procesie gromadzenia lub przetwarzania informacji.
7. Czy w zakładzie ubezpieczeń rejestrowane są zdarzenia/działania w systemach informatycznych (serwery, bazy

danych, aplikacje, systemy operacyjne) wykorzystywanych do przetwarzania danych i informacji (wrażliwych, chronionych i istotnych dla zakładu ubezpieczeń), takie jak:

- działania autoryzowanych użytkowników;
- działania nieautoryzowanych użytkowników;
- awarie;
- alarmy systemowe;
- inne; mogące mieć wpływ na przetwarzane dane i informacje (poufność, integralność, dostępność).

8. Czy w systemach informatycznych (serwery, bazy danych, aplikacje, systemy operacyjne) zaimplementowane zostały rozwiązania w zakresie autoryzacji, monitorowania dostępu do systemu i jego użycia. (PN-ISO/IEC 17799 i Rozporządzenia Ministra Spraw Wewnętrznych I Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych)
9. Czy środowiska produkcyjne, testowe i programistyczne systemów operacyjnych są logicznie oddzielone?
10. Czy do prac rozwojowych testowych i produkcyjnych używane są te same środowiska systemowe?
11. Czy dostęp do środowisk produkcyjnych, testowych i programistycznych systemów operacyjnych z poziomu administratora jest rozdzielany pomiędzy różne osoby?
12. Czy zdefiniowano zasady przenoszenia kodu pomiędzy środowiskami programistycznymi, testowymi i produkcyjnymi oraz role i odpowiedzialności do wykonywania tych operacji? Czy są one przestrzegane?
13. Czy w zakładzie ubezpieczeń rejestrowane są komunikaty systemowe (generowane przez systemy informatyczne), istotne dla monitorowania bezpieczeństwa?
14. Czy zakład ubezpieczeń posiada narzędzia uniemożliwiające administratorom systemów modyfikacje logów systemowych?
15. Czy możliwa jest sytuacja, w której przegląd dzienników systemowych i ewentualna ich modyfikacja dokonywany może być przez tą samą osobę, której działania są monitorowane?
16. Czy w zakładzie ubezpieczeń udzielane są specjalne przywileje pozwalające obejść zabezpieczenia systemów lub aplikacji?
17. Czy analizowany jest stopień wykorzystania infrastruktury informatycznej (zajętość dysków, wykorzystanie procesorów oraz pamięci operacyjnej?
18. Czy zakład ubezpieczeń posiada i wykorzystuje narzędzia antywirusowe? Jak często dokonuje ich aktualizacji?
19. Czy zakład ubezpieczeń posiada procedury tworzenia i odtwarzania kopii zapasowych w zależności od klasyfikacji danych?
20. Czy zostały określone warunki techniczne do bezpiecznego przechowywania kopii zapasowych?

21. Czy sieć zakładu ubezpieczeń jest monitorowana w zakresie ilości ruchu oraz identyfikacji działań podejrzanych?
22. Czy sieć telekomunikacyjna zakładu ubezpieczeń jest podzielona logicznie lub fizycznie na obszary związane z departamentami biznesowymi?
23. Czy w sieci zakładu ubezpieczeń zainstalowane są narzędzia monitorujące ruch sieci w szczególności urządzenia typu IDS (intrusion detection system)?
24. Czy w zakładzie ubezpieczeń ustalone i wdrożone są procedury określające zasady kopiowania, przechowywania i niszczenia danych i informacji (uwzględniające poszczególne typy nośników informacji)?
25. Czy w zakładzie ubezpieczeń ustalone są zasady bezpieczeństwa jakie powinny być zachowane przy przekazywaniu informacji i danych, min. w formie dokumentów, za pomocą telefonów (stacjonarnych i komórkowych), przy pomocy poczty głosowej, za pośrednictwem poczty elektronicznej, przy pomocy urządzeń faksowych i czy pracownicy przeszli szkolenie w tym zakresie?
26. Czy są w zakładzie ubezpieczeń regulacje określające jakie informacje, oprogramowanie lub sprzęt (w tym nośniki zawierające dane np. twarde dyski, dyskietki, pamięci typu flash) mogą być wynoszone poza siedzibę?
27. Czy w zakładzie ubezpieczeń zostały określone i są przestrzegane warunki techniczne (np. szyfrowanie dysków w laptopach) umożliwiające bezpieczne przetwarzanie danych i informacji poza siedzibą zakładu, jeśli zaistnieje taka konieczność?
28. Czy w zakładzie ubezpieczeń ustalone i wdrożone są procedury określające sposób przechowywania lub niszczenia nośników (np. dokumentacja papierowa, twarde dyski, dyskietki), które nie będą już dalej wykorzystywane?
29. Czy udzielone przywileje są ewidencjonowane, w sposób pozwalający zidentyfikować osobę wyrażającą zgodę na udzielenie takich przywilejów i powód ich udzielenia?
30. Czy zakład ubezpieczeń posiada procedury dotyczące poczty elektronicznej, zwłaszcza określające zakres i sposób przekazywania informacji mających szczególne znaczenie dla zakładu ubezpieczeń?.
31. Czy serwer poczty elektronicznej jest monitorowany programem antywirusowym, czy blokowany jest ruch poczty elektronicznej z niedozwolonymi załącznikami?

Bezpieczeństwo logiczne eksploatowanych systemów sieciowych i systemów informatycznych

1. Czy przy określaniu dostępu do informacji poszczególni użytkownicy mają „zablokowany dostęp jedynie do informacji nie przeznaczonych dla nich" czy też „wszystkie informacje są zablokowane, a tylko niezbędne są udostępnione"?
2. Czy w zakładzie ubezpieczeń obowiązuje formalny proces rejestracji użytkownika systemu informatycznego?
3. Czy użytkownik systemu informatycznego otrzymując dostęp do odpowiednich zasobów otrzymuje pisem-

ne potwierdzenie nadania uprawnień i potwierdza poprzez złożenie podpisu na kopii, zrozumienie warunków dostępu?

4. Czy zostały określone zasady postępowania z identyfikatorami pracowników długotrwale (pow. 30 dni) nieobecnych w pracy?
5. Czy zostały określone i wdrożone zasady przekazywania informacji do komórki odpowiedzialnej za blokowanie uprawnień dotyczące odchodzących pracowników?
6. Czy w przypadku gdy pracownik zmienił stanowisko lub odszedł z pracy niezwłocznie odbierane są prawa dostępu i dokonywane są odpowiednie adnotacje w rejestrze użytkowników systemu?
7. Czy użytkownicy systemu informatycznego mają przydzielany unikalny identyfikator użytkownika, czy są używane identyfikatory grupowe?
8. Czy w zakładzie ubezpieczeń istnieje formalny zakaz ponownego użycia, przydzielonych wcześniej, identyfikatorów do systemu informatycznego?
9. Czy w zakładzie ubezpieczeń istnieje procedura nadawania dostępu do systemów informatycznych z poziomu administratora? Czy tworzona w związku z tym prowadzona dokumentacja pozwala określić min. kto, kiedy i w jakim zakresie otrzymał uprawnienia administracyjne?
10. Czy w zakładzie ubezpieczeń dokonywane są, w sposób formalny, okresowe przeglądy udzielonych praw dostępu?
11. Czy uzyskując dostęp do urządzeń komputerowych lub systemów informatycznych oprócz identyfikatora konieczne jest podanie osobistego hasła?
12. Czy system wymusza zmianę początkowego hasła oraz cykliczną zmianę użytkowanego hasła?
13. Czy pracownicy przeszkoleni zostali w zakresie tworzenia i zabezpieczenia (**w tym zakazu udostępniania !!!**) hasła osobistego?
14. Czy w przypadku konieczności wydania hasła tymczasowego jest ustalona procedura weryfikacji tożsamości użytkownika zwracającego się z prośbą o wydanie takiego hasła?
15. Czy pracownicy zakładu ubezpieczeń mają zdalny dostęp (np. za pomocą Internetu) do zasobów informacyjnych zakładu ubezpieczeń, zgromadzonych w systemach komputerowych (w tym także do serwerów pocztowych)?
16. Czy zdalny dostęp pracowników do zasobów zakładu ubezpieczeń jest zabezpieczony poprzez szyfrowanie połączenia? Czy do procesu autoryzacji wykorzystywane są hasła modyfikowane poprzez urządzenia typu „token”?
17. Czy, gdy zakład ubezpieczeń za pomocą urządzeń technicznych, udostępnia swoje informacje na zewnątrz (także własnym pracownikom), określone są w sposób formalny warunki bezpieczeństwa jakie powinny być zachowane w takich sytuacjach?
18. Czy w przypadku stwierdzenia naruszeń systemów informatycznych ustalany jest i w sposób formalny wprowa-

dzany w życie, sposób postępowania pozwalający przeciwdziałać podobnym przypadkom?

19. Czy rozpoczynając pracę w systemach informatycznych użytkownik informowany jest w wyraźny sposób, w jakiej części systemu („testowej" czy „produkcyjnej") rozpoczął pracę?
20. Czy możliwa jest sytuacja, w której udzielony zostanie dostęp do zasobów informacyjnych bez wiedzy „właściciela" tych zasobów?

Rozwijanie i utrzymanie systemów sieciowych i systemów informatycznych

1. Czy nowe urządzenia, wykorzystywane do przetwarzania danych i informacji, przechodzą proces autoryzacji, tzn. czy weryfikowane są pod kątem zabezpieczeń jakie obowiązują w zakładzie ubezpieczeń?
2. W jaki sposób następuje formalne dopuszczenie do użytku nowych urządzeń komputerowych?
3. Czy nowy sprzęt lub oprogramowanie przed dopuszczeniem do użytkowania weryfikowane jest po kątem zgodności z dotychczasowymi składnikami systemu?
4. W jaki sposób następuje formalne dopuszczenie do użytku nowych programów?
5. Czy aktualizacja użytkowanego oprogramowania dokonywana jest tylko przez wskazanego w sposób formalny pracownika czy też aktualizacji takiej dokonać może samodzielnie użytkownik?
6. Czy przed dokonaniem aktualizacji oprogramowania użytkownik aplikacji wyraża na to każdorazowo formalną zgodę?
7. Czy aktualizacje oprogramowania są rejestrowane w sposób pozwalający zidentyfikować min. datę dokonanej aktualizacji i wersję nowego i starego oprogramowania?
8. Czy po dokonaniu aktualizacji oprogramowania zachowywana jest jego poprzednia wersja?
9. Czy aktualizacje oprogramowania zawsze dokonywane są po sprawdzeniu jej poprawności działania w „bazie testowej"?
10. Czy w testach uczestniczą użytkownicy końcowi?
11. Czy w testach wykorzystywane są prawdziwe dane pochodzące z „bazy produkcyjnej"?
12. Czy w zasobach zakładu ubezpieczeń zachowywana jest dokumentacja dotycząca testów nowej wersji oprogramowania?
13. Czy w zakładzie ubezpieczeń prowadzony jest rejestr kodów źródłowych używanego oprogramowania umożliwiający min. identyfikację osób mających dostęp do tych kodów?
14. Czy dostęp do kodów źródłowych mają wszyscy programiści, czy też udostępniane są one na podstawie specjalnego pozwolenia?
15. Czy w bazach „testowych" i „produkcyjnych" można korzystać z tych samych haseł osobistych?

Zgodność z przepisami obowiązującego prawa

1. Czy zakład ubezpieczeń dokonał inwentaryzacji regulacji prawnych dotyczących przetwarzania w nim danych i informacji?
2. Czy oprogramowanie wykorzystywane przez zakład ubezpieczeń ma uregulowane prawa własności intelektualnej?
3. Czy środki zastosowane do ochrony określonych danych i informacji są zgodne z przedmiotowymi regulacjami zewnętrznymi?
4. Czy okresy przechowywania określonych danych i informacji są zgodne z przedmiotowymi regulacjami zewnętrznymi?
5. Czy zakład ubezpieczeń przewidział sankcje w przypadku korzystania przez pracowników ze środków przetwarzania danych i informacji w sposób nieautoryzowany?
6. Czy zakład ubezpieczeń przewidział cykliczną weryfikację zgodności dokumentacji systemowej oraz konfiguracji systemów w odniesieniu do polityki bezpieczeństwa.

Członkowie Podkomisji ds. Audytu i Kontroli Wewnętrznej Komisji Ekonomiczno-Finansowej Polskiej Izby Ubezpieczeń biorący udział w opracowaniu programów audytu:

Jolanta Antczak

Ewa Kornacka

Joanna Pietrusiewicz

Monika Rosa

Beata Sambora

Elżbieta Szambelan-Bakuła

Anna Wawrzeniecka

Agnieszka Żmijewska

Krzysztof Kozłowicz

Krzysztof Łochański

Tomasz Pietrzak

Robert Popadyniec

Bogusław Rajca

Wojciech Stasiak

Tomasz Wiącek

Piotr Piórek – sekretarz

Polska Izba Ubezpieczeń

ul. Wspólna 47/49,
00-684 Warszawa
www.piu.org.pl