PLANOWANIE AWARYJNE W PRAKTYCE BANKOWEJ

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

Piotr Truszczyński
Departament Inspekcji Bankowych
Warszawa, 31 stycznia 2019 roku

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

Planowanie awaryjne w praktyce bankowej – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- Planowanie awaryjne
- Testy planów
- Działania proaktywne
- Działania kontrolne
- Przyczyny nieprawidłowości
- Podsumowanie

Planowanie awaryjne w praktyce bankowej – agenda spotkania

- **Definicje, wymogi prawne i regulacyjne**
- Planowanie awaryjne
- Testy planów
- Działania proaktywne
- Działania kontrolne
- Przyczyny nieprawidłowości
- Podsumowanie

Definicje, wymogi prawne i regulacyjne

BCM (Business Continuity Management) system zarządzania ciągłością działania (zasoby ludzkie, podział zadań, procedury utrzymania / odtworzenia, zasoby awaryjne)

BCP (Business Continuity Planning plany utrzymania ciągłości działania) na wypadek awarii i zdarzeń operacyjnych o ograniczonym zasięgu, o przewidywalnym przebiegu

Awaria – niesprawność urządzenia i / lub systemu IT, skutkująca jego unieruchomieniem, wadliwym działaniem lub niedostępnością, może dotyczyć pojedynczych lub kilku obiektów (rozległa awaria), przewidywalny zakres i skala działań naprawczych, możliwa stosunkowo szybka naprawa i przywrócenie stanu pierwotnego

Katastrofa – zdarzenie występujące zazwyczaj w wyniku działania czynnika zewnętrznego, możliwe zagrożenia dla zdrowia i życia, gwałtowny i nieprzewidywalny przebieg, rozległy charakter uszkodzeń, niedostępność infrastruktury technicznej, długotrwały proces usuwania skutków, trudna do szybkiego oszacowania skala działań naprawczych, konieczność wykorzystania zasobów rezerwowych w dużym zakresie

Definicje, wymogi prawne i regulacyjne

Krytyczne procesy – wskazane przez bank procesy w obrębie jego działalności, w przypadku których szybkie odzyskanie sprawności działania może mieć istotne znaczenie z punktu widzenia ciągłości działania instytucji

Tolerancja/apetyt na ryzyko – … ryzyka, na które instytucja jest gotowa i które jest skłonna podjąć a priori (apetyt na ryzyko), jak i faktyczne limity w ramach tego apetytu, jakie instytucja sobie wyznacza …

Profil ryzyka operacyjnego – skala i struktura ekspozycji na ryzyko operacyjne; określa stopień narażenia na ryzyko operacyjne i może być wyrażony w wybranych przez bank wymiarach strukturalnych (takich jak m.in. rodzaje zdarzeń operacyjnych, rodzaje linii biznesowych, kluczowe procesy) oraz wymiarach skali (takich jak m.in. oszacowana potencjalna wielkość straty); do jego ustalenia bank wykorzystuje m.in. posiadane informacje na temat zdarzeń operacyjnych (w tym dotyczące ich częstości i dotkliwości) oraz informacje pochodzące z wykorzystywanych narzędzi zarządzania ryzykiem operacyjnym

Definicje, wymogi prawne i regulacyjne

Banki mają obowiązek identyfikowania i zarządzania poszczególnymi rodzajami ryzyka prowadzonej działalności

Ryzyko braku ciągłości działania – stanowi jeden z istotnych czynników ryzyka operacyjnego

Planowanie awaryjne w obszarze IT ma na celu ograniczenie skutków materializacji ryzyka braku ciągłości działania, stanowi uzupełnienie procesu zarządzania mającego na celu zapobieganie występowaniu sytuacji awaryjnych, realizowanego obszarze IT głównie poprzez

- zarządzanie bieżącą eksploatacją środowiska IT oraz jego zabezpieczeniami
- zapewnienie skalowalności, wydajności, pojemności komponentów IT
- zarządzanie rozwojem infrastruktury (wdrożenie, zmiany w środowisku IT)
- testowanie przedwdrożeniowe, testy bezpieczeństwa i ciągłości działania
- proces zarządzanie incydentami (wykrywanie i wczesne reagowanie)

Definicje, wymogi prawne i regulacyjne (ustawa Prawo bankowe)

Ustawa Prawo bankowe

Art. 6c. 1. Powierzenie przez bank wykonywania stale lub okresowo czynności, o których mowa w art. 6a ust. 1, może nastąpić po spełnieniu następujących warunków:

1) bank i przedsiębiorca lub przedsiębiorca zagraniczny będą posiadać plany działania zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową

Art. 9b. 1. Zadaniami systemu zarządzania ryzykiem są identyfikacja, pomiar lub szacowanie, kontrola oraz monitorowanie ryzyka występującego w działalności banku służące zapewnieniu prawidłowości procesu wyznaczania i realizacji szczegółowych celów prowadzonej przez bank działalności.

Definicje, wymogi prawne i regulacyjne (ustawa Prawo bankowe)

2. W ramach systemu zarządzania ryzykiem bank:

1) stosuje sformalizowane zasady służące określaniu wielkości podejmowanego ryzyka i zasady zarządzania ryzykiem;
2) stosuje sformalizowane procedury mające na celu identyfikację, pomiar lub szacowanie oraz monitorowanie ryzyka występującego w działalności banku, uwzględniające również przewidywany poziom ryzyka w przyszłości;
2) stosuje sformalizowane limity ograniczające ryzyko i zasady postępowania w przypadku przekroczenia limitów;
3) stosuje przyjęty system sprawozdawczości zarządczej umożliwiający monitorowanie poziomu ryzyka;
4) posiada strukturę organizacyjną dostosowaną do wielkości i profilu ponoszonego przez bank ryzyka.

Definicje, wymogi prawne i regulacyjne (uchwała 258 / 2011 KNF)

UCHWAŁA NR 258/2011 KOMISJI NADZORU FINANSOWEGO z dnia 4.10.2011 r. w sprawie szczegółowych zasad funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz szczegółowych warunków szacowania przez banki kapitału wewnętrznego i dokonywania przeglądów procesu szacowania i utrzymywania kapitału wewnętrznego oraz zasad ustalania polityki zmiennych składników wynagrodzeń osób zajmujących stanowiska kierownicze w banku

(Zastąpiona przez Rozporządzenie MRiF z 6.03.2017 r.)

Definicje, wymogi prawne i regulacyjne (uchwała 258 / 2011 KNF)

(par 13 pkt 8) … bank wprowadza w szczególności: w zakresie ryzyka operacyjnego:

- procedury zarządzania ryzykiem operacyjnym … uwzględniające zdarzenia charakteryzujące się niską częstotliwością występowania, lecz wysokimi stratami
- **plany utrzymania ciągłości działania** zapewniające ciągłe i niezakłócone działanie banku oraz plany awaryjne służące zapewnieniu możliwości prowadzenia bieżącej działalności banku i ograniczeniu strat w przypadku wystąpienia niekorzystnych zdarzeń wewnętrznych i zewnętrznych mogących poważnie zakłócić tę działalność
- **zasady zarządzania kadrami**, w tym rekrutacji, monitorowania potrzeb kadrowych oraz planowania zaplecza kadrowego (kadry rezerwowej)
- **zasady zarządzania ryzykiem powierzenia wykonywania czynności podmiotom zewnętrznym**

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

Rozporządzenie Ministra Rozwoju i Finansów z 6.03.2017 r. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, polityki wynagrodzeń oraz szczegółowego sposobu szacowania kapitału wewnętrznego w bankach (wybrane zagadnienia)
(obowiązuje od 1 maja 2017 r.)

Organizacja systemu zarządzania ryzykiem
§ 3.1 system zarządzania ryzykiem i kontroli wewnętrznej są zorganizowane na trzech niezależnych poziomach:

1. zarządzanie ryzykiem w działalności operacyjnej banku
2. zarządzanie ryzykiem przez niezależne komórki ds. ryzyka oraz działalność komórki do spraw zgodności
3. działalność komórki audytu wewnętrznego

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

§ 8 (zadania zarządu)

projektowanie i wprowadzenie systemu zarządzania ryzykiem

- strategia zarządzania ryzykiem, polityki, procedury wewnętrzne
- limity
- nadzorowanie wielkości i profilu ryzyka z uwzgl. podm. zależnych
- ustalenie zasad raportowania
- nadzorowanie zarządzania (poziomy 1 i 2)

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

§ 37 (komórka zgodności)

Zapewnienie zgodności procedur, procesów, organizacji z przepisami prawa, regulacjami wewnętrznymi, standardami rynkowymi (identyfikowanie, monitorowanie, ocena szacowanie / pomiar ryzyka braku zgodności oraz wprowadzanie mechanizmów kontrolnych i raportowanie na potrzeby zarządu i rady nadzorczej - szczegóły powinny zostać określone w regulaminie)

§ 38 (audyt wewnętrzny)

Badanie procesu zarządzania ryzykiem, dostosowanie planów audytu do poziomu istotności ryzyka, kontrola realizacji zaleceń, raporty dla zarządu i rady nadzorczej

Zgodnie z § 39 ust. 11 i 12, pracownicy komórek (zgodności i audytu wewnętrznego) nie mogą wykonywać innych zadań niż wynikających z zadań ww. komórek

Przepisu ust. 12 (komórka zgodności) nie stosuje się do banków spółdzielczych zrzeszonych w bankach zrzeszających

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

§ 10 (rada nadzorcza)

nadzór nad wprowadzeniem, ocena adekwatności i skuteczności systemu zarządzania ryzykiem

- zatwierdzenie (określonego przez zarząd) akceptowalnego ogólnego poziomu ryzyka oraz jego monitorowanie
- zatwierdzenie przyjętej przez zarząd strategii zarządzania ryzykiem oraz monitorowanie przestrzegania
- nadzór nad politykami i procedurami systemu zarządzania ryzykiem
- nadzór nad wykonywaniem obowiązków przez zarząd
- określenie zasad raportowania do rady nadzorczej o rodzajach i wielkości ryzyka w działalności
- ocena adekwatności i skuteczności systemu zarządzania ryzykiem

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

§ 12. metody identyfikowania i pomiaru / szacowania, kontroli ryzyka, monitorowania i raportowania o ryzku oraz częstotliwość są uzależnione od wielkości i profilu ryzyka

§ 13. bank przeprowadza testy warunków skrajnych

§ 14. bank stosuje limity, (wysokość zatwierdza zarząd)

- wysokość limitów jest dostosowana do ogólnego poziomu ryzyka (rada)

- analizy wysokości limitów są odpowiednio dokumentowane

§ 17. system sprawozdawczości zarządczej, wspomagający proces decyzyjny

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

§ 18. bank wprowadza polityki i procedury w zakresie ryzyka operacyjnego

- zasady zarządzania ryzykiem operacyjnym (definicje, rejestracja, monitorowanie strat, zdarzenia o niskiej częstotliwości i wysokich stratach, ryzyko prawne) … uwzględniające zdarzenia charakteryzujące się niską częstotliwością występowania, lecz wysokimi stratami
- plany utrzymania ciągłości działania (niezakłócone działanie) i plany awaryjne na wypadek zdarzeń (wewnętrznych i zewnętrznych) mogących **poważnie** zakłócić działalność
- zasady zarządzania kadrami (planowanie i monitorowanie zaplecza kadrowego)
- **zasady zarządzania ryzykiem systemów, związanych z prawidłowym, efektywnym i bezpiecznym wspieraniem działalności banku przez jego środowisko teleinformatyczne**
- zasady zarządzania ryzykiem powierzenia czynności podmiotom zewnętrznym

Definicje, wymogi prawne i regulacyjne (Rozporządzenie MRiF)

§ 22 nadzór nad ryzykiem związanym z działalnością podmiotów zależnych:

- zgodny z przyjętą przez bank strategią zarządzania ryzykiem
- uwzględnia rodzaj prowadzonej działalności
- uwzględnia zasady określone w § 18
- uwzględnia ocenę wielkości i profilu ryzyka podmiotów zależnych

Definicje, wymogi prawne i regulacyjne (Rekomendacja M KNF)

Ogólny zakres planowania awaryjnego określa ***Rekomendacja M KNF dotycząca zarządzania ryzykiem operacyjnym w bankach***

Rekomendacja 11

Bank powinien posiadać system zarządzania ciągłością działania, w tym plany utrzymania ciągłości działania oraz plany awaryjne, zapewniający nieprzerwane działanie banku na określonym poziomie, uwzględniającym profil ryzyka operacyjnego banku

plany utrzymania ciągłości działania zapewniające ciągłe i niezakłócone działanie banku,

plany awaryjne służące zapewnieniu możliwości odtworzenia działalności banku i ograniczeniu strat w przypadku wystąpienia niekorzystnych zdarzeń wewnętrznych i zewnętrznych zakłócających tą działalność

11.2 identyfikacja procesów krytycznych (definicje, analizy)

4.13 zasady zarządzania systemami informatycznymi z uwzględnieniem planów awaryjnych (istotność, krytyczność)

4.28 plany awaryjne dla procesów realizowanych przez podmioty zewnętrzne (bank - podmiot)

4.31 umowy z podmiotami zewnętrznymi (wymagane czynności)

Definicje, wymogi prawne i regulacyjne (Rekomendacja D KNF)

Rekomendacja D KNF dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach

(działania zapobiegawcze)
Rekomendacja 5
Rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego banku powinny być adekwatne do jego profilu ryzyka i specyfiki działalności oraz pozwalać na efektywną realizację działań w tych obszarach
- Zapewnienie adekwatnej struktury organizacyjnej, podziału zadań, zasobów ludzkich

Rekomendacja 9
Bank powinien posiadać sformalizowane **zasady dotyczące zarządzania infrastrukturą teleinformatyczną**, w tym jej architekturą, poszczególnymi komponentami, wydajnością i pojemnością oraz dokumentacją, zapewniające właściwe wsparcie działalności banku oraz bezpieczeństwo przetwarzanych danych
- zapewnienie parametrów ograniczających możliwość powstawania awarii i incydentów

Rekomendacja 13 (wsparcie użytkowników)
Bank powinien zapewniać wewnętrznym użytkownikom systemów informatycznych wsparcie w zakresie rozwiązywania problemów związanych z ich eksploatacją, w tym wynikających z wystąpienia awarii i innych niestandardowych zdarzeń zakłócających ich użytkowanie
- zapewnienie możliwości szybkiego reagowania w celu ograniczenia zasięgu ew. awarii

Definicje, wymogi prawne i regulacyjne (Rekomendacja D KNF)

Rekomendacja 15 (dostosowanie systemu zarządzania ciągłością działania)
System zarządzania ciągłością działania banku powinien uwzględniać szczególne uwarunkowania związane z jego środowiskiem teleinformatycznym oraz przetwarzanymi w nim danymi

Plany utrzymania ciągłości działania
15.1. zgodność z Rekomendacją M KNF
15.2 komitet BCM / BCP w złożonych organizacjach
15.3 ciągłość działania jednostek i środowiska IT (podstawa innych planów BCP)
15.4 dokumentacja BCP IT (klasyfikacja systemów)
15.5 system dystrybucji planów awaryjnych (dostępność, aktualność)
15.6 uwzględnienie dostawców zewnętrznych (komunikacja, testy, dostawcy alternatywni)

Zasoby techniczne
15.7 adekwatne zasoby IT **(bieżące funkcjonowanie i odtworzenie),** z uwzględnieniem zdefiniowanych procesów (max czas odtworzenia i utraty danych)

Definicje, wymogi prawne i regulacyjne (Rekomendacja D KNF)

15.8, 15.9 ośrodki zapasowe (lokalizacja, funkcjonalność)
15.10 – 15.14 bezpieczeństwo fizyczne zasobów IT, udokumentowana analiza zagrożeń, weryfikacja zabezpieczeń

Kopie awaryjne
15.15 klasyfikacja zasobów, schemat kopiowania (częstotliwość, zakres)
15.16 weryfikacja kopii (kompletność, jakość)
15.17, 15.18 procedury tworzenia kopii, zasady ewidencji
15.19 zabezpieczenie kryptograficzne danych na nośnikach zewnętrznych
15.20 likwidacja zbędnych kopii i nośników (ochrona przed nieuprawnionym dostępem)

Weryfikacja efektywności podejścia do zarządzania ciągłością działania
15.21 zasady testowania, zakres testów (adekwatność), scenariusze

Definicje, wymogi prawne i regulacyjne (Rekomendacja D KNF)

Rekomendacja 18

W banku powinien funkcjonować sformalizowany, skuteczny system zarządzania bezpieczeństwem środowiska teleinformatycznego, obejmujący działania związane z identyfikacją, szacowaniem, kontrolą, przeciwdziałaniem, monitorowaniem i raportowaniem ryzyka w tym zakresie, zintegrowany z całościowym systemem zarządzania ryzykiem i bezpieczeństwem informacji w banku

- zarządzanie bezpieczeństwem działania proaktywne - mitygowanie

Rekomendacja 20

Bank powinien posiadać sformalizowane zasady zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego, obejmujące ich identyfikację, rejestrowanie, analizę, priorytetyzację, wyszukiwanie powiązań, podejmowanie działań naprawczych oraz usuwanie przyczyn

- zarządzanie incydentami, ograniczanie skali ew. awarii

Definicje, wymogi prawne i regulacyjne (Rekomendacja D KNF)

Rekomendacja 21

Bank powinien zapewnić zgodność funkcjonowania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z wymaganiami prawnymi, regulacjami wewnętrznymi i zewnętrznymi, zawartymi umowami i przyjętymi w banku standardami

- (zgodność z regulacjami, komórka zgodności)

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

Planowanie awaryjne w praktyce bankowej – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- **Planowanie awaryjne**
- Testy planów
- Działania proaktywne
- Działania kontrolne
- Przyczyny nieprawidłowości
- Podsumowanie

Planowanie awaryjne – profil ryzyka

Główne czynniki kształtujące profil ryzyka braku ciągłości działania banku

- charakter działalności (uniwersalny, specjalistyczny)
- skala działalności (liczba klientów, rachunków, produktów, suma bilans. etc)
- skala transakcji realizowanych elektronicznymi kanałami obsługi, liczba serwisów, usług, udostępnionych produktów
- złożoność środowiska teleinformatycznego (liczba maszyn, systemów operacyjnych i bazodanowych, urządzeń sieciowych, aplikacji, kont administratorów i użytkowników, niewspieranych komponentów, etc.)
- wsparcie zarządzania środowiskiem teleinformatycznym (automatyzacja)
- skala realizowanych zmian (fuzje, przejęcia, rozwój środowiska IT)
- złożoność struktury organizacyjnej (zmiany w strukturze organizacyjnej, obsada i rotacja zatrudnienia)
- charakter powiązań z podmiotami zewnętrznymi, udział w grupach bankowych
- zakres i charakter wykorzystania usług zewnętrznych IT (outsourcing)

Planowanie awaryjne – źródła informacji

Źródła informacji w procesie planowania awaryjnego

- rejestr zdarzeń i strat operacyjnych (definicje zdarzeń, wsparcie IT, szkolenia, struktura, rekoncyliacja strat, opóźnienia rejestracji, „ciemna liczba")
- rejestr incydentów bezpieczeństwa i zdarzeń w systemach IT
- analizy ryzyka (proces BIA, monitorowanie SLA, odczyt wskaźników KPI / KRI, mapy ryzyka)
- analizy (scenariuszowe i statystyczne zdarzeń i strat operacyjnych)
- analizy ryzyka systemów teleinformatycznych (poufność, integralność, dostępność, niezaprzeczalność, rozliczalność)
- wyniki testów ciągłości działania i testów bezpieczeństwa
- wyniki kontroli wewnętrznej (kompletność i skuteczność mechanizmów kontrolnych)
- wyniki procesu audytu wewnętrznego
- inne źródła, analiza zdarzeń (przypadki zewnętrzne), etc.

Planowanie awaryjne – proces BIA

Proces BIA (Business Impact Analysis) – identyfikacja procesów i zasobów niezbędnych do udostępnienia produktu / usługi

- definiowanie i identyfikacja procesów i zasobów
- klasyfikacja procesów i zasobów (krytyczne i pozostałe, kryteria klasyfikacji)
- ocena i szacowanie skutków braku ciągłości działania procesu / zasobu (wymiar czasowy i finansowy)
- identyfikacja właścicieli i wykonawców procesu, właścicieli zasobów
- określenie minimalnych zasobów (ludzkich, systemowych lokalowych etc.),
- testy procedur awaryjnych dla poszczególnych procesów / zasobów
- standaryzacja kart procesów (systematyka, wsparcie, analizy)
- mapowanie zagrożeń dla procesów, wskaźniki ryzyka
- samoocena ryzyka, analiza ekspercka (zaangażowanie komórek organizacyjnych realizujących procesy krytyczne)
- przegląd i aktualizacja procesu BIA
- prezentacja wyników procesu BIA dla kierownictwa – decyzje zarządcze

Planowanie awaryjne – elementy procesu

Główne elementy procesu planowania awaryjnego

- identyfikacja i analiza zagrożeń (aktualizacja, proces ciągły)
- założenia BCM / BCP, (limity ogólne, limity niedostępności zasobów IT i procesów)
- identyfikacja, klasyfikacja, zasobów krytycznych (lokalizacje, komórki organizacyjne / pracownicy etc.)
- analiza adekwatności obsady (liczba zatrudnionych, kompetencje, szkolenia) usługodawcy zewnętrzni (dostępność, jakość)
- klasyfikacja systemów (identyfikacja krytycznych) i danych (dostępność jakość i kompletność kopii awaryjnych)
- analiza adekwatności zasobów awaryjnych: lokalizacja, infrastruktura techniczna, moc obliczeniowa i pojemność, sieć teleinformatyczna, Internet, zasilanie awaryjne, ochrona, etc.
- struktura zarządzania awaryjnego, odpowiedzialność, koordynacja, (komitet)
- dokumentacja – kompletność, aktualność, dystrybucja (dostępność)

Planowanie awaryjne – szczegółowość

Wybrane czynniki wpływające na szczegółowość planów awaryjnych

- charakter dokumentu, adresaci dokumentu (strategia, polityka, procedura)
- rodzaje identyfikowanych czynników ryzyka i zagrożeń
- struktura organizacyjna (liczba zatrudnionych), podział zadań (specjalizacja)
- przygotowanie merytoryczne, dostępność, rotacja pracowników
- wyposażenie techniczne (awaryjne), charakter ośrodków przetwarzania
- automatyzacja procesu odtworzeniowego
- skala wykorzystania usług zewnętrznych, specyfika i jakość usług, dostępność dostawców alternatywnych
- inne

Planowanie awaryjne – struktura

Struktura planów (procedur) awaryjnych

- informacja o statusie dokumentu, (data zatwierdzania, okres aktualizacji …)
- definicje, okoliczności i kompetencje i zasady aktywowania planu
- kompetencje w zakresie koordynacji i zarządzania wykonaniem planu
- listy kontaktowe (komunikacja)
- wymagane niezbędne zasoby awaryjne (ludzkie, techniczne IT, proceduralne)
- priorytety, kolejność realizacji działań, opis czynności scenariusze (część merytoryczna)
- zasady działania w trybie awaryjnym oraz powrotu do stanu sprzed awarii
- częstotliwość, zakres testowania i raportowania

Planowanie awaryjne – struktura

Struktura zarządzania awaryjnego

- członek zarządu (zarząd) bezpośrednio odpowiedzialny za proces BCM
- komitet BCM / KRO (koordynacja działań na szczeblu departamentów banku na etapie planowania, opracowania procedur, testów)
- sztab antykryzysowy (na wypadek aktywowania planu awaryjnego)
- koordynatorzy procesu w komórkach organizacyjnych (IT oraz komórkach merytorycznych)
- pracownicy komórek organizacyjnych odpowiedzialni za wykonanie procedur awaryjnych oraz wyznaczone zastępstwa

Planowanie awaryjne – etapy procesu

Główne etapy procesu

I etap - akcja ewakuacyjna i ratownicza (ochrona życia i zdrowia)

- identyfikacja zagrożeń (urządzenia wspierające detekcję zdarzeń)
- powiadamianie pracowników, klientów i służb ratowniczych (urządzenia alarmowe, komunikacja, łączność)
- automatyczne systemy ochrony (zasilanie, automatyczne gaszenie, oddymianie)
- ewakuacja (systemy dostępu, windy, oświetlenie awaryjne, bramki etc.)
- miejsce zbiórek, ustalenie liczby poszkodowanych (nieobecnych)

Planowanie awaryjne – etapy procesu

Główne etapy procesu

II etap (po zakończeniu akcji ratowniczej)

- zabezpieczenie dokumentów i danych
- zabezpieczenie mienia
- zabezpieczenie materiału dowodowego (np. zapis video, rejestratory, etc.)
- ocena skutków zdarzenia
- powiadomienie odpowiednich instytucji zewnętrznych (media)
- ustalenie priorytetów w zakresie likwidacji skutków zdarzenia
- powiadomienie usługodawców i dostawców, ubezpieczycieli

Planowanie awaryjne – etapy procesu

Główne etapy procesu

III etap - odtworzenie działalności (plan awaryjny)

- zapewnienie łączności i bieżącej informacji (w tym dla klientów)
- ustalenie priorytetów i harmonogramu działań (procedury awaryjne)
- udostępnienie zasobów awaryjnych (lokalizacje zastępcze, procedury odtworzeniowe, sprzęt, systemy IT, awaryjne kopie danych)
- odtworzenie środowiska teleinformatycznego w zasobach awaryjnych
- odtworzenie konfiguracji, uprawnień użytkowników i danych z kopii
- uruchomienie testowe systemów i aplikacji
- kontrola poprawności działania systemów i aplikacji
- udostępnienie środowiska produkcyjnego dla pracowników i klientów (w oparciu o zasoby awaryjne)
- odtworzenie środowiska podstawowego
- powrót systemów i procesów do stanu sprzed awarii, katastrofy

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

Planowanie awaryjne w praktyce bankowej – agenda spotkania

- Definicje
- Wymogi prawne i regulacyjne
- Planowanie awaryjne
- **Testy planów**
- Działania proaktywne
- Działania kontrolne
- Przyczyny nieprawidłowości
- Podsumowanie

Testy planów

Testy planów BCP

- określenie zakresu i częstotliwości testów (analizy BIA, ryzyka, etc.)
- plan testów (budżet), zatwierdzenie, wykonanie, organizacja, zabezpieczenia
- scenariusze testów (wybrane komponenty IT, lokalizacje, kompleksowe przełączanie środowisk – warunki wykonania)
- udział podmiotów zewnętrznych (usługodawców) i podmiotów zależnych
- analizy wyników testów vs. przyjęte założenia, RTO, SLA, BIA
- udział pracowników komórek merytorycznych
- raportowanie wyników testów (protokoły KRO, zarząd, RN)
- ocena zdolności banku do utrzymania ciągłości działania krytycznych procesów i usług w przypadku wystąpienia awarii
- ocena zdolności banku do odtworzenia działalności w przypadku wystąpienia rozległych awarii i katastrof (zdolność do szybkiego uruchomienia i prowadzenia działalności w oparciu o zapasowy ośrodek przetwarzania)
- decyzje i działania zarządcze

Testy planów – wybrane scenariusze

Wybrane scenariusze awaryjne

- sytuacje zagrażające życiu i zdrowiu ludzi (wybuch, katastrofa budowlana, pożar, awarie elektryczne)
- niedostępność krytycznych lokalizacji (centrala banku, kluczowe oddziały)
- niedostępność kluczowych pracowników
- niedostępność głównych zasobów (ośrodki przetwarzania) – przełączenie środowisk IT
- awarie komponentów systemów utrzymania środowiska fizycznego (zasilanie elektryczne, klimatyzacja, dostęp i ochrona, video, p. poż., etc.)
- awarie poszczególnych, centralnych komponentów środowiska IT, WAN / LAN / GSM, Internet
- niedostępność istotnych oddziałów (regionalne, specjalistyczne)
- incydenty bezpieczeństwa IT: ataki wirusowe, malware, hakerskie, (Dos/DDoS), wyciek danych wrażliwych
- masowe ataki przeciwko klientom korzystającym z systemów bankowości elektronicznej

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

Planowanie awaryjne w praktyce bankowej – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- Planowanie awaryjne
- Testy planów
- **Działania proaktywne**
- Działania kontrolne
- Przyczyny nieprawidłowości
- Podsumowanie

Działania proaktywne

Elementy ograniczające występowanie zdarzeń i ich skutków

- monitorowanie ryzyka operacyjnego (KRI, KPI / SLA) – wczesne sygnały,
- monitorowanie jakości procesu BCP (aktualność i zakres planów, zakres i wyniki testów, etc.)
- wczesna identyfikacja problemów IT, awarii, błędów, incydentów, systemy wspierające (IDS, SIEM)
- linie obrony (help desk, komórki typu SOC, inne rodzaje wsparcia)
- stosowanie redundantnych rozwiązań i środowisk teleinformatycznych (zasoby awaryjne działające w czasie rzeczywistym)
- standaryzacja środowisk, efektywne zarządzanie architekturą, zmianą, rozwojem, incydentami
- technika wirtualizacji, automatyzacja procesu kopiowania i odtworzenia środowiska, centralne repozytoria (dostępność kopii awaryjnych)
- repozytoria dokumentacji systemowej i awaryjnej, bazy CMDB
- kompleksowy proces testowania i działania naprawcze (wyniki testów)
- wybór lokalizacji i lokalizacji zastępczych dla ośrodków przetwarzania
- rezerwy kadrowe, szkolenia BCP, udział w testach usługodawców

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

Planowanie awaryjne w praktyce bankowej – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- Planowanie awaryjne
- Testy planów
- Działania proaktywne
- **Działania kontrolne**
- Przyczyny nieprawidłowości
- Podsumowanie

Działania kontrolne

Wybrane elementy kontroli wewnętrznej i audytu

Kontrola wewnętrzna
- formalizacja planów awaryjnych, zasad przeglądu i aktualizacji planów
- podział zadań i odpowiedzialności (karty zadań, procedury)
- rejestracja zdarzeń i strat operacyjnych
- weryfikacja poprawności analiz, map ryzyka, informacji zarządczej BIA
- kontrola procesów / czynności realizowanych przez podmioty zewnętrzne

Komórka zgodności: zgodność procesu BCM / BCP z regulacjami i przepisami

Audyt wewnętrzny
- częstotliwość i zakres badań (uwzględnienie zagrożeń i wyników testów)
- wsparcie specjalistyczne (m. inn. skuteczność stosowanych rozwiązań)
- niezależna ocena jakości procesu planowania awaryjnego BCM / BCP
- monitorowanie wykonania zaleceń
- niezależne raportowanie na potrzeby zarządu i rady nadzorczej

Rola zarządu i rady nadzorczej – decyzje zarządcze i nadzorcze

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

Planowanie awaryjne w praktyce bankowej – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- Planowanie awaryjne
- Testy planów
- Działania proaktywne
- Działania kontrolne
- **Przyczyny nieprawidłowości**
- Podsumowanie

Przyczyny nieprawidłowości

Wybrane czynniki zwiększające ryzyko dla realizacji procesu BCM

- niekompletne i lub nieaktualne procedury wewnętrzne (zakres merytoryczny, podział kompetencji decyzyjnych, listy kontaktowe, podział zadań, etc..)
- nieadekwatne zasoby ludzie (obsada, rotacja, przygotowanie merytoryczne)
- jakość usług świadczonych przez podmioty zewnętrzne na rzecz banku, brak udziału w testach
- brak wystarczających zasobów awaryjnych (wydajność, pojemność, dostępność komponentów IT, lokalizacje)
- brak testów planów i procedur awaryjnych (zakres, scenariusze, częstotliwość)
- niewystarczająca kontrola i audyt (zakres, częstotliwość)
- niski priorytet procesu BCM / BCP w strategii banku oraz decyzjach zarządczych

Przyczyny nieprawidłowości

Identyfikowane nieprawidłowości w trakcie inspekcji

1. **W zakresie proceduralnym**

- brak podziału zadań i kompetencji pomiędzy członków komitetu BCP i komitetu awaryjnego (lub brak aktualizacji)
- brak określenia zasad i częstotliwości przeglądu (aktualizacji planu)
- brak planów ciągłości działania dla wszystkich procesów krytycznych
- brak uwzględnienia w BCP scenariuszy w ataków np. DDoS
- brak procedur odtworzenia środowiska IT w lokalizacji zapasowej
- brak określenia maksymalnego dopuszczalnego czasu przywrócenia procesów krytycznych oraz zorganizowania środowiska awaryjnego
- rozbieżności parametrów ciągłości działania w poszczególnych dokumentach procesu BCM / BCP
- brak planów ciągłości działania dla oddziałów
- brak ujęcia w procedurach zasad weryfikacji planów awaryjnych usługodawcy zewnętrznego
- brak koordynacji planów awaryjnych banku z planami usługodawcy

Przyczyny nieprawidłowości

2. **W zakresie organizacyjnym**
- brak wskazania osób / komórek odpowiedzialnych za koordynację procesu BCP (poza IT)
- brak prezentacji na posiedzeniach zarządu, wyników testów BCP

3. **W zakresie funkcjonalnym**
- niewystarczający zakres testów BCP (wybrane elementy procesu biznesowego / wybrane systemy krytyczne), brak objęcia testami systemu wyliczania BFG
- niewystarczająca częstotliwość testów BCP / brak testów planu awaryjnego
- brak potwierdzenia możliwości kompleksowego odtworzenia działalności w ośrodku alternatywnym (brak testów przełączeniowych)
- brak centrum zapasowego, brak możliwości szybkiego odtworzenia środowiska w alternatywnej lokalizacji

Monitoring

Liczba i czas awarii

Systemy informatyczne (ogółem)

-max: 128

-min: 0

Systemy krytyczne

-max: 61

-min: 0

Czas niedostępności systemów krytycznych (godz.)

-max: 2 251

-min: 0

*Dane (Urzędu KNF) na podstawie ankiet z banków komercyjnych (I Q 2018)

KNF | CEDUR Centrum Edukacji dla Uczestników Rynku

Planowanie awaryjne w praktyce bankowej – agenda spotkania

- Definicje, wymogi prawne i regulacyjne
- Planowanie awaryjne
- Testy planów
- Działania proaktywne
- Działania kontrolne
- Przyczyny nieprawidłowości
- **Podsumowanie**

Podsumowanie

Ewolucja planów awaryjnych, dostosowanie planów BCP do zmian specyfiki ryzyka działania banków (wybrane czynniki)

- proces łączenia banków, zmiany w środowiskach teleinformatycznych
- zmiana charakteru działania banków, rosnąca skala usług elektronicznych, malejąca liczba oddziałów,
- automatyzacja („robotyzacja") procesów sprzedaż, back office, obsługa IT
- wirtualizacja, usługi współdzielone (cloud computing)
- rosnący udział usługodawców zewnętrznych w obszarze IT i procesach biznesowych
- zagrożenia ze strony cyberprzestępczości (ataki kierowane przeciwko bankom, pracownikom i klientom)

Podsumowanie

Dziękuję za uwagę

Piotr Truszczyński