



— Praktyczny przewodnik

ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA

SIERPIEŃ 2014



Instytut Auditorów
Wewnętrznych
IIA POLSKA



The Institute of
Internal Auditors

Global

Spis treści

Streszczenie.....	1
Wstęp.....	2
Role i zobowiązania audytu wewnętrznego	4
Główne elementy zarządzania ciągłością działania w ocenie audytu wewnętrznego.....	5
Działania audytu wewnętrznego przed sytuacją kryzysową	7
Działania audytu wewnętrznego w trakcie sytuacji kryzysowej i po jej zakończeniu.....	7
Aneks	9
Autorzy i recenzent.....	23

Streszczenie

Zarządzanie ciągłością działania (BCM) pozwala organizacjom przygotować się na incydenty lub sytuacje kryzysowe mogące przeszkodzić w osiągnięciu celów biznesowych. Zarządzanie kryzysowe (CM), to główny element BCM mający na celu przekazywanie istotnych informacji na temat sytuacji kryzysowej interesariuszom organizacji.

Dzięki szerokiemu zakresowi kompetencji i kwalifikacji, pozycji w organizacji oraz dogłębnej wiedzy na temat operacji zachodzących w organizacji, audyt wewnętrzny może znacząco przyczynić się do opracowania, wdrożenia oraz oceny inicjatyw związanych z BCM i CM podejmowanych przez organizację. Audyt wewnętrzny może odgrywać role zarówno kluczowe, jak i poboczne, w zależności od tego, czy inicjatywy dotyczące BCM i CM w ogóle istnieją i/lub od ich dojrzałości, jak również od powagi i okoliczności sytuacji kryzysowej.

Role audytu wewnętrznego, to m.in. usługi zapewniające oraz doradcze przed wystąpieniem sytuacji kryzysowej, w trakcie i po jej zakończeniu. Udzielanie zapewnienia oraz usługi doradcze wymagają doskonałej znajomości głównych elementów BCM, takich jak ład organizacyjny, zarządzanie ryzykiem, analiza wpływu na działalność BIA (Business Impact Analysis) oraz planowanie ciągłości działania i odtwarzania po awarii (BCRP).

- W celu weryfikacji skuteczności BCM i CM, można przeprowadzić działania zapewniające.
- Usługi doradcze pomagają kierownictwu skoncentrować się na planowaniu działań i skoordynowaniu BCM i CM z ryzykami i kontrolami.

Na potrzeby organizacji, w czasie sytuacji kryzysowej audytorzy wewnętrzni mogą zostać poproszeni i upoważnieni do sprawowania funkcji niezwiązanych z audytem.

Wstęp

Globalny Przewodnik Audytu Technologicznego IIA (GTAG) 10: Zarządzanie ciągłością działania omawia wagę zarządzania ciągłością działania (BCM), jest wartościowym źródłem informacji na temat głównych elementów skutecznego programu BCM oraz zawiera wskazówki dotyczące ciągłości działania głównych systemów infrastruktury IT oraz aplikacji biznesowych w trakcie sytuacji kryzysowej i po jej zakończeniu. Niniejszy praktyczny przewodnik szczegółowo opisuje zarządzanie ciągłością działania, przedstawiając potencjalne role audytora w zarządzaniu ryzykiem i zapewnianiu wytycznych dotyczących:

- działań audytu wewnętrznego przed wystąpieniem sytuacji kryzysowej, w trakcie i po jej zakończeniu.
- głównych elementów zarządzania ciągłością działania w ocenie audytu wewnętrznego.

Pomoce praktyczne znajdujące się w Aneksie, zawierają listę kontrolną oceny ryzyka, przykładowe programy audytowe, glosariusz oraz odniesienia.

Znaczenie procesów biznesowych oraz związane z nimi ryzyka

Wszystkie organizacje prędzej czy później muszą zmierzyć się z przerwami w prowadzeniu działalności. Odpowiednio ułożony plan BCM/CM jest dla organizacji niczym polisa ubezpieczeniowa pozwala mieć pewność, że organizacja pozostanie rentowna i nadal będzie spełniać oczekiwania interesariuszy. Ponadto, plany BCM/CM zapewniają audytowi wewnętrznemu miejsce stałego uaktualniania i komunikowania efektywnego zarządzania ryzykiem i kontroli ryzyka w organizacji.

Plany zarządzania kryzysowego (CMP) łączą w sobie środki zapobiegawcze i reaktywne zarządzanie ryzykiem w przypadku poważnych sytuacji kryzysowych.

Nieefektywne, błędnie sporządzone lub zakomunikowane plany zarządzania kryzysowego - w połączeniu z niewystarczającym testowaniem lub wyszkoleniem - mogą prowadzić do wzrostu poziomu ryzyka w organizacji z krytycznego do niedopuszczalnego.

Plany zarządzania kryzysowego opracowane po wystąpieniu sytuacji kryzysowej mogą zawierać luki, gdyż są opracowane na bazie ostatniego zdarzenia. Ich zawartość może być niewystarczająca, by być skuteczna. W przypadku organizacji z sektora publicznego, w tym administracji rządowej ryzyka wynikające z wystąpienia sytuacji kryzysowej lub incydentu mogą za sobą pociągać szersze konsekwencje, zarówno lokalne jak i międzynarodowe.

Odpowiednio przedstawiony oraz kompleksowy plan zarządzania kryzysowego może wesprzeć organizację w skutecznym działaniu podczas wystąpienia sytuacji kryzysowej i związanych z nią ryzyk. Ponadto, plan zarządzania kryzysowego może zwiększyć odporność organizacji w obliczu sytuacji kryzysowej. Narzędzia i programy zarządzania kryzysowego, jeśli są tworzone mądrze, sprawdzane okresowo oraz zalecane i zatwierdzane przez kierownictwo i/lub zarząd, umożliwią organizacjom zarządzanie zdarzeniami i ograniczanie ryzyk celem zminimalizowania ogólnych ryzyk operacyjnych, finansowych, utraty reputacji oraz prawnych, na które narażeni są kluczowi wewnętrzni i zewnętrzni interesariusze.

Standardy i wytyczne IIA

Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego (Standardy) dotyczące BCM i CM to między innymi:

Standard 2100: Charakter pracy

Stosując systematyczne i uporządkowane podejście, audyt wewnętrzny musi dokonywać oceny i przyczyniać się do usprawniania procesów: ładu organizacyjnego, zarządzania ryzykiem i kontroli.

Standard 2110: Ład organizacyjny

Audyt wewnętrzny musi oceniać procesy kształtujące ład organizacyjny i przedstawiać stosowne zalecenia usprawnienia tych procesów, tak by osiągnąć następujące cele:

- promowanie odpowiednich zasad etyki i wartości w organizacji;
- zapewnienie skutecznego zarządzania efektywnością działań organizacji i odpowiedzialności za wyniki;
- przekazywanie informacji o ryzykach i kontroli do odpowiednich obszarów organizacji oraz
- koordynowanie działań i przekazywanie informacji pomiędzy radą, audytorami zewnętrznymi i wewnętrznymi oraz kierownictwem.

Standard 2120: Zarządzanie ryzykiem

Audyt wewnętrzny musi oceniać skuteczność i przyczyniać się do usprawnienia procesów zarządzania ryzykiem.

Standard 2400: Informowanie o wynikach

1. Audytorzy wewnętrzni muszą informować o wynikach zadań.

Definicje kluczowych pojęć

BCM - zarządzanie ciągłością działania to proces, dzięki któremu organizacja przygotowuje się na przyszłe incydenty lub sytuacje kryzysowe mogące zagrozić podstawowej misji organizacji oraz jej krótko- i długoterminowej zdolności do ciągłości działania oraz sprostania oczekiwaniom interesariuszy. CM, uważane za główny element BCM, mówi o tym, jak organizacja powinna informować opinię publiczną, swych pracowników, partnerów biznesowych oraz interesariuszy o klęsce lub sytuacji kryzysowej oraz krokach podjętych celem przywrócenia działalności biznesowej i zminimalizowania wpływu na wewnętrznych i zewnętrznych interesariuszy. Plany zarządzania kryzysowego (CMP), to skonsolidowane portfolio czynności składających się z zapobiegawczych oraz reaktywnych działań, jakie każda organizacja powinna

wykonać, by skutecznie zarządzać i minimalizować ryzyka powstałe na skutek sytuacji kryzysowej lub zdarzenia.

Zarządzanie ciągłością działania

BCM - zarządzanie ciągłością działania, to sposób zarządzania ryzykiem oparty na wartości biznesowej, dostarczający zdolność ciągłości działania do ryzyk. Celem BCM jest umożliwienie organizacji przywrócenia krytycznych działań operacyjnych, zarządzania informacjami oraz zminimalizowania finansowych i innych efektów katastrofy, zakłócenia działalności oraz innych poważnych zdarzeń. BCM polega na zarządzaniu ryzykiem w taki sposób, by stworzyć zdolność ciągłości działania, które odpowiadałyby możliwym ryzykom, w oparciu o wartości biznesowe.

Choć terminologia w literaturze fachowej może się różnić, termin BCM - zarządzanie ciągłością działania - opisuje w niniejszym przewodniku ogólną politykę/ model/ ramy zarządzania różnymi typami przerw w dostarczaniu usług, które mogą zostać wywołane przez zdarzenia wewnętrzne lub zewnętrzne względem organizacji. Definicję tę można również stosować w organizacjach sektora publicznego, takich jak organizacje rządowe. W przypadku takich organizacji termin „biznes” oznacza instytucje rządowe, podstawową działalność publiczną, bezpieczeństwo publiczne oraz ochronę obywateli.

Główne elementy BCM to:

- **Wsparcie kierownictwa** – kierownictwo udziela wsparcia, by odpowiednio przygotować, utrzymać i wykonać plan ciągłości działania (BCP) poprzez przydzielenie odpowiednich zasobów, ludzi oraz środków z budżetu.
- **Oszacowanie i ograniczanie ryzyka** – określane są potencjalne ryzyka wynikające z zagrożeń takich, jak pożar czy powódź, oraz ich prawdopodobieństwo i potencjalny wpływ na organizację. Dokonuje się tego na miejscu, na poziomie oddziału, tak by zagwa-

rantować, że ryzyka związane z wszystkimi możliwymi zdarzeniami są zrozumiałe i odpowiednio zarządzane.

- **Analiza BIA - analiza wpływu na działalność** – identyfikuje procesy biznesowe stanowiące nieodłączny element utrzymania funkcjonowania jednostki biznesowej w sytuacji klęski oraz określa, jak szybko integralne procesy powinny zostać wznowione po jej wystąpieniu.
- **Wznowienie działalności oraz strategia ciągłości** – wskazuje konkretne kroki, ludzi oraz zasoby potrzebne do wznowienia podstawowych procesów biznesowych. Identyfikuje również kluczowe mechanizmy i protokoły informacyjne. Strategia może zawierać wzorce i standardy danej firmy lub sektora.
- **Znajomość planu i szkolenie** – szkolenie z zakresu BCP oraz wiedza na jego temat są niezbędne do zarządzania ciągłością działania. Szkolenie może również składać się z wykonywania ćwiczeń i/lub rozpatrywania praktycznych zagadnień dotyczących fragmentów planu ciągłości działania.
- **Utrzymanie, obsługa, konserwacja** – podtrzymywane są zdolność i dokumentacja BCM, tak by pozostały skuteczne oraz zgodne z priorytetami biznesowymi.

CM - zarządzanie kryzysowe

CM to główny element BCM, który zostaje uruchomiony, gdy zakłócenie usługi biznesowej dochodzi do poziomu sytuacji kryzysowej lub sytuacji awaryjnej. CM dokumentuje metody wykorzystywane w odpowiedzi na rzeczywistość i postrzeganie sytuacji kryzysowych.

CM polega również na określeniu wskaźników celem zdefiniowania scenariuszy sytuacji kryzysowych oraz mechanizmów, jakie powinny zostać w takiej sytuacji uruchomione. Zarządzanie kryzysowe (CM) polega na komunikowaniu następującym w fazie reagowania na scenariusz zarządzania awaryjnego.

Typy zakłóceń

BCM dąży do zarządzania zarówno zagrożeniami wewnętrznymi, jak i zewnętrznymi. Zagrożenia w różnym stopniu odbijają się na procesach biznesowych organizacji, co może negatywnie wpływać na przestrzeganie uregulowań, bezpieczeństwo personelu, ochronę środowiska, możliwość utrzymania standardów działania, spełnianie wymogów umowy oraz na markę/reputację organizacji. Wśród typów zakłóceń znajdują się:

- Ataki cybernetyczne.
- Choroby/pandemia.
- Trzęsienie ziemi/tsunami.
- Pożar.
- Powódź.
- Huragan/tornado.
- Przerwanie pracy.
- Awaria/przestój produkcji.
- Skażenie produktu.
- Sabotaż.
- Przerwa w dostawie usług lub produktów przez kluczowych partnerów biznesowych/dostawców.
- Awaria systemu.
- Terroryzm.
- Przerwa w dostawie mediów.

Role i zadania audytu wewnętrznego

Definiowanie roli audytu wewnętrznego

Zadaniem audytorów wewnętrznych jest włączenie się w zarządzanie sytuacją kryzysową poprzez przekazywanie organizacjom praktycznych spostrzeżeń na temat działań. Zarządzający audytem wewnętrznym powinien zdefiniować rolę audytu wewnętrznego przed, w trakcie i po zakończeniu sytuacji kryzysowej, uważając, by nie przejść obowiązków związanych z odpowiedzialnością za ryzyka w sytuacji kryzysowej lub zarządzaniem nimi. Audyt wewnętrzny często obecny jest w procesie planowania zarządzania sytuacją kryzysową. Po pierwsze, zarządzający audytem wewnętrznym wraz z najważniejszymi członkami kierownictwa audytu wewnętrznego powinni zapoznać się z głównymi praktykami BCM poprzez odniesienia zewnętrzne i standardy. Materiały znajdują się w Pomocach praktycznych III niniejszego praktycznego przewodnika. Po określeniu ról, należy je udokumentować i przekazać pracownikom audytu wewnętrznego oraz głównym interesariuszom zewnętrznym, których sprawa dotyczy bezpośrednio.

Jeśli role audytora wewnętrznego lub zarządzającego audytem wewnętrznym nie zostaną określone w procesie zarządzania kryzysowego, należy powiadomić o tym komitet audytu, by uniknąć rozminięcia się oczekiwań. Kiedy audyt wewnętrzny pełni rolę doradczą wobec kierownictwa w kontekście opracowania BCP/CMP, należy wziąć pod uwagę problem potencjalnego wpływu na niezależność i obiektywność audytu wewnętrznego. Kiedy role zostaną określone, powinny one zostać zatwierdzone przez zarządzającego audytem wewnętrznym. Jednocześnie administracyjne i funkcjonalne struktury raportowania powinny zostać opisane, zatwierdzone oraz potencjalnie udokumentowane w karcie audytu wewnętrznego.

Zadania doradcze i zapewniające związane z BCM

Obowiązek audytora wewnętrznego odnoszący się do przysparzania wartości oraz usprawniania operacji organizacji i działań dotyczących zarządzania ryzykiem powinien również obejmować zadania doradcze i zapewniające związane z BCM, w zależności od dojrzałości programu BCM danej organizacji. Włączenie działań audytu wewnętrznego do procesu planowania lub ulepszania BCM i CM może być kluczowym elementem zapewniającym powodzenie programu. Jest tak szczególnie w przypadku organizacji o niskim poziomie dojrzałości w tym obszarze.

Biorąc pod uwagę fakt, iż audyt wewnętrzny analizuje i rozumie potrzeby zarządu i kierownictwa wykonawczego organizacji, może on zapewnić perspektywę oraz pomóc skoncentrować się na czynnościach związanych z planowaniem. Zapewnienie zgodności kluczowych obszarów BCM z potrzebami zarządu i kierownictwa wykonawczego jest niezbędne, by osiągnąć sukces.

Zadania zapewniające

Audyt wewnętrzny może przeprowadzać okresowe działania zapewniające celem sprawdzenia, czy BCP i CMP są kompleksowe i istotne dla aktualnego biznesowego otoczenia operacyjnego oraz czy poinformowano o nich odpowiednich wewnętrznych i zewnętrznych interesariuszy. Częstotliwość, charakter oraz zakres wykonywanych prac będą zależać od ryzyk oraz próśb interesariuszy o sprawdzenie skuteczności i znaczenia zaplanowanych działań.

W zakres działań zapewniających może wchodzić kompleksowy program BCM lub jego poszczególne elementy (np. weryfikacja częstotliwości występowania i uaktualniania BCP, oraz dojrzałości CMP). Wiedza audytu wewnętrznego na temat ryzyk zminimalizowanych przez BCP lub CMP oraz wcześniejsze zaangażowanie w działania doradcze w trakcie opracowywania planów mogą przyczynić się do stworzenia skuteczniejszego procesu planowania zadań.

Do zadań zapewniających należą:

- Prośby o dokonanie przez komitet audytu lub kierownictwo wykonawcze przeglądu programu BCM lub jego elementów, w tym audytu dostawców lub partnerów biznesowych.
- Przeglądy BCM w celu dokonania oceny jego kompletności, dojrzałości i trafności w oparciu o ryzyka organizacyjne, rozwój lub transakcje zbycia.
- Oceny ryzyka programu.
- Przeglądy istniejących zapisów BCP/CMP organizacji lub partnera biznesowego określonych w warunkach umowy (tj. klauzul dotyczących prawa do przeprowadzania audytu lub określonych umów o poziomie świadczonych usług SLA¹).

Dodatkowe wytyczne dotyczące programów zadań zapewniających znajdują się w Pomocach praktycznych I.

Zadania doradcze

Ponieważ dostęp do danych oraz ich transfer uważane są za podstawowe funkcje w biznesie, przedmiotem zainteresowania BCM może szybko stać się przegląd i analiza infrastruktury IT. Jednakże świadcząc usługi doradcze w zakresie BCM/CM audyt wewnętrzny powinien uwzględniać szerokie spektrum celów i ryzyk organizacyjnych, i nie ograniczać głównych założeń zadania do kwestii związanych z IT. Zadania doradcze w zakresie BCM nie powinny zagrażać obiektywizmowi audytu wewnętrznego. Należy uważać, by nie przejąć obowiązków związanych z odpowiedzialnością za ryzyka dotyczące ciągłości działania oraz zarządzanie nimi.

¹) Service Level Agreement (SLA) – umowa o gwarantowanym poziomie świadczenia usług – umowa utrzymania i systematycznego poprawiania ustalonego między klientem a usługodawcą poziomu jakości usług. Zadaniem umowy wsparcia typu SLA jest świadczenie usług, których celem jest zapewnienie ciągłości istotnych procesów.

Główne elementy zarządzania ciągłością działania w ocenie audytu wewnętrznego

Programy BCM zawierają pospolite elementy takie jak ład organizacyjny, zarządzanie ryzykiem, analiza BIA oraz planowanie ciągłości działania i odtwarzania po awarii (BCRP). Bardzo ważne jest, by w każdy z tych elementów zaangażowani byli odpowiedni gwaranci, interesariusze oraz partnerzy biznesowi, by wspomóc opracowanie kompleksowego, cieszącego się poparciem oraz wykonalnego planu. Ogólne elementy komunikacyjne w ramach planów oraz informacje na ich temat należy przekazywać głównym interesariuszom. Działania audytu wewnętrznego mogą obejmować ocenę skuteczności BCM i CMP.

Ład organizacyjny

Kluczem do skutecznego zarządzania ciągłością działania jest wsparcie oraz patronat kierownictwa zarządzającego. Audyt wewnętrzny może pomóc w określeniu i nawiązaniu relacji między głównymi wewnętrznymi interesariuszami BCM. Na początkowym etapie oceny BCM audyt wewnętrzny może wykonać następujące czynności:

- Określić, czy pozycje głównych osób zarządzających zostały udokumentowane i zatwierdzone, by pomóc zapewnić odpowiedzialność za programy organizacji i ich wiarygodność.
- To głównie do osób zarządzających należy identyfikacja współzależności planu, promowanie ciągłego ulepszania oraz wyciąganie wniosków z działań podejmowanych po zakończeniu sytuacji kryzysowej. Należy:
- Rekomendować rozszerzenia karty BCM. Karta pomaga ustalić patronat i wsparcie dla programu wewnątrz najwyższych struktur w organizacji. Jasno zdefiniowana karta, oprócz poświadczenia istnienia programu BCM, określa strukturę ładu organizacyjnego BCM (tj. komitet BCM) oraz wytyczne dotyczące

ce okresowej oceny karty. Struktura ładu organizacyjnego zatwierdza decyzje BCM lub CM i zapewnia podgląd rozwoju BCP lub CMP w całej organizacji, jak również przeglądów oraz powiązanej wewnętrznej i zewnętrznej komunikacji.

- Ocenić, czy ustalona struktura ładu organizacyjnego BCM i CM jest odpowiednio finansowana, właściwa i efektywnie służy potrzebom zarządu, komitetu audytu lub kierownictwa zarządzającego. Audyt wewnętrzny może odgrywać rolę członka bez prawa głosu, lub brać udział w spotkaniach w celu przekazywania uwag na temat roli, karty oraz działań takiej jednostki.
- Przekazywać informacje oraz doradzać na temat tego, czy ład organizacyjny BCM odpowiednio i skutecznie wypełnia potrzeby zarządu, komitetu audytu i kierownictwa zarządzającego.
- Powiadamiać zarząd (komitet audytu) o ryzykach i najlepszych praktykach dotyczących ciągłości działania i planów zarządzania kryzysowego.

Zarządzanie ryzykiem

Aby BCM było skuteczne, musi brać pod uwagę najistotniejsze ryzyka, w obliczu których staje organizacja w momencie wystąpienia sytuacji kryzysowej. Audyt wewnętrzny posiada często szczegółową wiedzę na temat podstawowych ryzyk biznesowych. W czasie sytuacji kryzysowej waga ryzyk może się zmieniać w oparciu o charakter i zakres zdarzeń dotykających organizację.

Audyt wewnętrzny może udzielać informacji na temat głównych ryzyk organizacyjnych w trakcie ustanawiania i oceniania BCM.

Znajomość głównych ryzyk dotyczących BCM może pomóc lepiej opracować proponowany plan audytu wewnętrznego. Kontakt z działaniami z zakresu BCM organizacji pomaga audytorowi wewnętrznemu zidentyfikować główne obszary zagrożenia, w tym charakter/wsparcie organizacyjne, działania związane z kontrolą operacyjną oraz podstawowe procesy i zależności sys-

temów/danych/dostawców. Słabe punkty lub niepowodzenia w powyższych obszarach mogą sprawić, iż zespół audytu wewnętrznego skoncentruje swe zasoby na wykonywaniu zadań zapewniających i doradczych mających na celu dodanie wartości oraz usprawnienie działań organizacji. Gromadzenie danych o ryzyku pozwala kierować planem audytu wewnętrznego, a samemu audytowi pozwala dokonywać analiz celem oceny prawdopodobieństwa wystąpienia ryzyka, wpływów, kompleksowości i wiarygodności. Przykładowa lista kontrolna oceny ryzyka znajduje się w Pomocach praktycznych.

Analiza BIA

Audyt wewnętrzny może przekazać zalecenia co do tego, jak kierownictwo powinno przeprowadzić analizę BIA będącą głównym elementem BCM. Analiza BIA wspomaga identyfikację kluczowych aktywów przedsiębiorstwa, funkcji, aplikacji, partnerów, dostawców, zasobów oraz końcową ocenę potencjalnych strat organizacji w przypadku wystąpienia sytuacji kryzysowej. GTAG 10: Zarządzanie ciągłością działania zawiera przydatne wskazówki dotyczące przeprowadzania analizy BIA. Jej wyniki z pewnością podniosą poziom akcji zapobiegawczych, zakresu działań oraz gotowości do podejmowania ryzyka przez organizację. Jeśli analiza BIA zostanie przeprowadzona efektywnie, wskaże decydujące operacje, zasoby oraz procesy - obiekty, personel i technologię (w tym bezpieczeństwo logiczne i fizyczne) - i może wreszcie określić priorytety inwestycyjne dla planu ciągłości działania i powiązanego z nim planu zarządzania kryzysowego.

Planowanie ciągłości działania i odtwarzania po awarii (BCRP)

BCRP wskazuje proaktywną metodę, dzięki której organizacje mogą określić środki do utrzymania ciągłości biznesowej i naprawcze, w celu zarządzania i ograniczania głównych ryzyk organizacyjnych wywoływanych przez sytuację kryzysową. Audyt wewnętrzny może świadczyć usługi doradcze lub zapewniające związane z BCRP.

Działania audytu wewnętrznego przed sytuacją kryzysową

Ocena BCM, a w szczególności planu zarządzania kryzysowego, dokonana przez audyt wewnętrzny, pozwala upewnić się, że plan zarządzania kryzysowego pozostanie istotny dla priorytetów organizacyjnych w przypadku wystąpienia sytuacji kryzysowej.

Poniżej znajdują się typowe działania, w które można zaangażować audyt wewnętrzny przed wystąpieniem sytuacji kryzysowej:

- Dzielenie się wiedzą na temat rozwoju BCM z kierownictwem zarządzającym i komitetem audytu.
- Rozpatrzenie BCM jako ryzyka zagrażającego organizacji oraz wzięcie pod uwagę ryzyk rezydualnych przy opracowywaniu rocznego planu audytu.
- Ocena kluczowych umów z partnerami biznesowymi pod względem warunków umowy, w tym umów o poziomie świadczonych usług, klauzul dotyczących prawa do przeprowadzenia audytu oraz wymaganego raportowania do kierownictwa w kwestii środowiska systemu kontroli wewnętrznej u partnera.
- Doradzanie kierownictwu w kwestiach związanych z dokonywaniem ocen ryzyka BCM lub analiza trafności samooceny ryzyka BCM dokonanej przez kierownictwo.
- Wykonywanie zadań zapewniających związanych z BCP i/lub CMP w ramach rocznego planu audytu. Działania zapewniające mogą składać się z oceny elementów planu, przekazywania protokołów w ramach planu oraz aspektów operacyjnych planu.
- Jeśli role BCM dla audytu wewnętrznego i zarządzającego audytem wewnętrznym nie zostały wcześniej ujęte w zapisach karty audytu wewnętrznego lub w wytycznych zarządu, należy je sprecyzować i ustanowić.

Działania audytu wewnętrznego w trakcie sytuacji kryzysowej i po jej zakończeniu

Poniższe punkty opisują powszechne działania, jakie audyt wewnętrzny może przeprowadzić w czasie trwania sytuacji kryzysowej i po jej zakończeniu.

W trakcie sytuacji kryzysowej należy:

- Monitorować i ocenić reakcję organizacji na zdarzenie oraz być aktywnym członkiem zespołu zarządzania kryzysowego.
- Monitorować szczegóły awarii na potrzeby kolejnych audytów.
- Zasiadać w Komitecie zarządzania kryzysowego, by mieć pewność, że ryzyka związane z sytuacją kryzysową są zrozumiałe oraz, jeśli zajdzie taka potrzeba, przekazać kierownictwu zalecenia co do alternatywnych trybów postępowania.
- W szerszym zakresie uczestniczyć w zarządzaniu kryzysowym i procesie odtworzeniowym organizacji, według zatwierdzonych uzgodnień.

Standardy zezwalają na tego typu zaangażowanie pod warunkiem, że szczegóły dotyczące potencjalnego naruszenia niezależności audytu wewnętrznego zostaną ujawnione odpowiednim stronom (np. komitetowi audytu i kierownictwu BCM). Zaangażowanie audytu wewnętrznego może być większe na początkowym etapie sytuacji kryzysowej, kiedy to niezwykle potrzebne jest wsparcie dla ograniczonych zasobów organizacji.

Po zakończeniu sytuacji kryzysowej należy:

- Ocenić skuteczność działań odtworzeniowych organizacji i sporządzić raport.
- Kontynuować ocenę ryzyka, przekazać zalecenia oraz pomóc opracować działania mające na celu doskonalenie działalności.

- Dokonać przeglądów pokryzysowych, by wskazać możliwości działań dla BCM, a w szczególności dla rozwoju CMP.
- Wykonać zadania zapewniające, by ocenić, czy kierownictwo dokonało analizy przyczyn źródłowych i odpowiednio przeanalizowało jej wyniki, by uaktualnić BCP i CMP, jeśli zajdzie taka potrzeba. Uczestniczyć w procesie odtworzeniowym w całej organizacji według zatwierdzonych uzgodnień dotyczących BCP i CMP.

Działania te zostaną omówione w dalszej części niniejszego przewodnika.

Przeprowadzenie audytu procesów odtworzeniowych i skuteczność planu

Plan odtwarzania utraconych zasobów, jako element BCM, może wymagać od audytu wewnętrznego przeprowadzenia audytu procesów odtworzeniowych. W takim przypadku dodatkowa praca powinna zostać zawarta we wstępnej wersji planu i może prowadzić do zmiany jego priorytetów.

Ponadto, jeśli taka rola nie została przypisana, zarządzający audytem wewnętrznym powinien rozważyć, czy po dokonaniu oceny ryzyka należy zalecić zespołowi kierownictwa BCP przeprowadzenia audytu poszczególnych aspektów przywracania danych i/lub CMP.

Wśród działań kontrolnych, jakie można przedsięwziąć znajdują się:

- Kompleksowy przegląd procesu odtworzeniowego (tj. sprawdzenie, czy był zgodny z planowanym procesem oraz czy plan był na tyle szczegółowy, by zapewnić rozwiązania pojawiających się problemów).
- Audyt skuteczności procesu odtworzeniowego, w tym wyniki mierzone w odniesieniu do określonych wskaźników lub elementów planu, jak również efektywne i terminowe informowanie wewnętrznych i ze-

wewnętrznych interesariuszy/partnerów biznesowych.

- Przegląd kontroli i procesów specjalnych wprowadzonych poza regularną strukturą kontroli oraz potencjalny wpływ na ryzyka operacyjne i finansowe w organizacji.
- Kontrola procesów przywracania danych kierownictwa, co może wiązać się z analizą kluczowych procesów uzgadniania danych, przeprowadzanych przez kierownictwo celem zapewnienia kompletności i dokładności danych.
- Przegląd aktualnych wersji BCP i CMP po wdrożeniu planów, w tym rekomendacje, które pozwolą na efektywne rozwinięcie planu. Dotyczy to również własnych planów działania audytu wewnętrznego.

Uczestniczenie w procesie odtworzeniowym w szerszym zakresie

Audytorzy wewnętrzni mogą zostać poproszeni przez kierownictwo organizacji o udzielenie dodatkowego wsparcia personelowi operacyjnemu, który wykonuje jedną z poniższych czynności:

- Pracuje przy procesie odtworzeniowym.
- W przypadku wystąpienia niedostępności systemów IT, pracuje nad przywróceniem stanu normalnego procesów biznesowych.
- Wykorzystuje określone procedury alternatywne, by wykonać działania, dla których normalne procesy zostały przerwane.

Dla zarządzającego audytem wewnętrznym ważne jest, by, zanim określona zostanie rola audytu wewnętrznego w BCP/CMP, wziąć pod uwagę wymagania zatwierdzone przez komitet audytu. Ponadto, kiedy pracownicy działu audytu wewnętrznego zostaną przydzieleni do pomocy przy zarządzaniu kryzysowym lub działaniach odtworzeniowych, przypisane im zadania powinny być wykonywane pod nadzorem kierownictwa operacyjnego. Aby chronić obiektywność, zarządzający audytem wewnętrznym

powinien przeanalizować zadania operacyjne wykonywane przez audytorów wewnętrznych i unikać przypisywania ich w przyszłości do zadań zapewniających audytu wewnętrznego w tym samym obszarze.

Aneks

Pomoce praktyczne I: Próbné programy pracy dla zadań zapewniających i doradczych BCM

Audyt wewnętrzny odgrywa ważną rolę dokonując niezależnego przeglądu ogólnej adekwatności zarządzania ciągłością działania. Wnikliwość i częstotliwość działań kontrolnych oraz raportowania powinny być dopasowane do wagi operacji. Choć zakres działań kontrolnych i wynik prac mogą się różnić, we wszystkich przypadkach muszą one obejmować niezależną i obiektywną ocenę skuteczności programu testowania. Audyt wewnętrzny powinien określić zasadność podstawowych założeń poczynionych podczas opracowywania programu testowania. Zasadność podstawowych założeń, jak również adekwatność testowego planu, scenariuszy, harmonogramów oraz raportów, powinny być oceniane z uwzględnieniem wielkości i złożoności danej organizacji,

znaczenia rodzaju działalności oraz ryzyka i wpływu możliwych zakłóceń działalności. Audyt wewnętrzny powinien również obserwować ćwiczenia testowe, by dokonać oceny środowiska kontroli w różnych lokalizacjach, sprawdzić wyniki, ocenić, czy wdrożono odpowiednie mechanizmy raportowania i eskalacji, i czy są one wykorzystywane, oraz ocenić, czy plany testowe są uaktualniane i odzwierciedlają wyniki poprzednich testów. Audyt bierze pod uwagę pięć powszechnych aspektów BCM:

1. Środowisko i strategię biznesowe.
2. Metodologia i strategia BCP.
3. Analiza wpływów na procesy biznesowe (ocena ryzyka i kontrole).
4. Plan procesu odtworzeniowego.
5. Wiedza, testowanie i szkolenie.

Przykład 1:

PRZYKŁADOWY PROGRAM PRAC BCM		
PODOBSZAR	ELEMENTY	MOŻLIWE KWESTIE
1. Środowisko i strategię biznesowe	Branża	1. Główne standardy BCM w branży.
		2. Wymogi prawne dla branży, w której firma działa.
		3. Historia słabych punktów charakterystycznych dla branży
		4. Wykaz określonych władz i organów (agencje zewnętrzne).
	Zależności zewnętrzne	1. Należy określić i rozważyć relacje z najważniejszymi partnerami biznesowymi oraz zależności interesariuszy (w tym głównych dostawców, sprzedawców oraz funkcji zleczanych na zewnątrz).
		2. Należy wskazać kontrakty z głównymi partnerami biznesowymi oraz umowy o poziomie świadczonych usług, główne zapisy winno się udokumentować.
		3. Prawa do przeprowadzania audytu zawarte w klauzulach umowy winny być okresowo wykorzystywane oraz powinno się otrzymywać Standardy SAS 70SSAE 16 lub równorzędne raporty partnerów biznesowych (tj. Działania oceniające system, w tym zdolności tworzenia kopii zapasowych i odzyskiwania danych oraz okresowe przeglądy bezpieczeństwa).

PRZYKŁADOWY PROGRAM PRAC BCM		
PODOBSZAR	ELEMENTY	MOŻLIWE KWESTIE
2. Powiązanie metodologii BCP ze strategią biznesową, operacyjną i finansową	Strategia biznesowa	1. BCP powinien opierać się na strategii biznesowej firmy.
		2. BCP powinien uwzględniać wszystkie istotne jednostki i najważniejsze działania.
	Strategia operacyjna/techniczna	1. Zintegrowane powinny być zarówno strategia operacyjna jak i IT.
		2. Przy podejmowaniu wszystkich istotnych decyzji biznesowych pod uwagę należy brać planowanie BCM.
		3. Obowiązki w zakresie BCP/CMP, w tym czynności utrzymujące powinny stanowić część obowiązujących opisów stanowisk i ocen personelu.
		4. BCP powinien być uaktualniany, rewidowany oraz testowany z częstotliwością odpowiednią dla ryzyk, podatności i wartości funkcji biznesowych.
	Strategia finansowa	1. Do przygotowania i utrzymania BCP powinny zostać udostępnione odpowiednie zasoby finansowe.
3. Analiza wpływu (w tym analiza BIA, ocena ryzyka oraz kontrole)	Postawa pracowników najwyższego szczebla	1. Zarząd oraz kierownictwo wyższego szczebla powinni wspierać inicjatywę BCM.
		2. Zadaniem personelu kierowniczego wyższego szczebla powinno być zapewnienie udanej implementacji, utrzymania oraz uaktualniania planów wspierających BCM.
		3. Powinna istnieć uaktualniana okresowo polityka/karta BCM.
		4. Plany związane z BCM, w tym BCP i CMP, powinny być zatwierdzane zarząd oraz odpowiednie organa kierownicze.
	Ocena ryzyka	1. Należy stworzyć kompleksową analizę BIA przygotowaną z myślą o danym rodzaju działalności.
		2. Różne typy zdarzeń, które mogłyby spowodować formalną deklarację o sytuacji kryzysowej lub katastrofie oraz proces uruchamiania BCP i CMP winny zostać wyczerpująco opisane.
		3. Jeśli kierownictwo uzna to za niezbędne, należy przeprowadzić analizę przepływu pracy i dokumentuje wyniki.
		4. Priorytetyzacja funkcji biznesowych powinna być odpowiednia.
		5. Ocena ryzyka winna obejmować ocenę wpływu i prawdopodobieństwa zakłóceń we wszystkich obszarach biznesowych, operacyjnych i IT oraz brać pod uwagę dopuszczalny czas zakłóceń.
		6. Powinny istnieć procedury realizacji priorytetów planów dla funkcji, usług i procesów krytycznych względem niekrytycznych.
		7. Skutki finansowe w przypadku wystąpienia sytuacji awaryjnej winny wiernie odzwierciedlać koszt w takim przypadku.
		8. Pod uwagę należy wziąć ryzyka utraty reputacji, a w analizie BIA - odpowiednich interesariuszy.

PRZYKŁADOWY PROGRAM PRAC BCM		
PODOBSZAR	ELEMENTY	MOŻLIWE KWESTIE
	Ograniczanie	1. Należy rozpatrzyć odpowiednie ograniczanie ryzyka, w tym strategię gotowości i prewencji, takie jak: a) Alternatywne lokalizacje i zdolność produkcyjna (zapewnienie różnorodności geograficznej). b) Zapewnione są zapasowe dane, aplikacje, telekomunikacja oraz inne potrzebne dane; istnieją również procedury. c) Kanały komunikacyjne w przypadku sytuacji awaryjnej są wyraźnie określone (drzewo komunikacyjne).
		2. Należy wskazać najważniejszych członków personelu i uaktualnić listę kontaktów.
		3. Pracownicy powinni rozumieć swoje role w przypadku sytuacji kryzysowej.
		4. Należy wskazać zapasowego dostawcę usług.
4. Plan odtworzeniowy	Wskaźnik docelowego punktu odzyskiwania (RPO) ²	1. Należy jasno zdefiniować i przedstawić wskaźniki RPO.
		2. Wskaźniki RPO powinny uwzględniać potrzeby odtworzeniowe organizacji.
	Wskaźnik przywracania działania w docelowym czasie (RTO) ³	1. Należy jasno zdefiniować i przedstawić wskaźniki RTO.
		2. Czas przywracania działania powinien należycie odzwierciedlać długość przestoju, jakie organizacja jest skłonna tolerować.
5. Świadomość, testowanie i szkolenie	Polityka testowania	3. Przy określaniu wskaźników RPO i RTO należy uwzględnić wyniki analizy BIA.
		1. W ramach BCP, organizacja ma wskazać wymagania dotyczące testowania funkcji ciągłości działania w całej organizacji, obszarów działania, funkcji wspierających oraz zarządzania kryzysowego.
		2. Polityka testowania powinna definiować kluczowe role i obowiązki.
		3. Należy zdefiniować cykle testowania o zwiększającym się zakresie i złożoności testów.

²⁾ RPO – Wskaźnik RTO (Recovery Time Objective - wskaźnik przywracania działania w docelowym czasie) – punkt w czasie, do którego systemy i dane muszą zostać przywrócone po przestoju (np. koniec działania poprzedniego dnia). Wskaźniki RPO są często wykorzystywane jako podstawa opracowania strategii tworzenia kopii zapasowych oraz do określenia ilości danych, które być może trzeba będzie odtworzyć po przywróceniu systemów lub funkcji.

³⁾ RTO – Wskaźnik przywracania działania w docelowym czasie (RTO - Recovery Time Objective) – okres, w którym systemy, aplikacje lub funkcje muszą zostać przywrócone po przestoju (zwykle jeden dzień roboczy). Wskaźniki RTO są często wykorzystywane jako podstawa opracowania strategii tworzenia kopii zapasowych oraz do określenia, czy strategię te zostaną wdrożone w trakcie sytuacji kryzysowej. Terminem zwykle związanym ze wskaźnikiem RTO jest maksymalny dopuszczalny czas przestoju.

Międzynarodowe Ramowe Praktyki Zawodowe (IPPF) – Praktyczny przewodnik Zarządzanie ciągłością działania

PRZYKŁADOWY PROGRAM PRAC BCM		
PODOBSZAR	ELEMENTY	MOŻLIWE KWESTIE
	Strategia testowania	1. Strategia testowania powinna zawierać udokumentowane plany testów oraz związane z nimi scenariusze, metody i harmonogramy testowania.
		2. Należy zdefiniować oczekiwania dotyczące testowania wewnętrznych i zewnętrznych zależności.
		3. Strategia testowania jest zgodna z założeniami i wymaganiami kierownictwa.
		4. BCP sprawdzany jest w rocznych lub częstszych cyklach testowania.
	Obserwacje dotyczące testowania	1. Testy należy przeprowadzać bez uprzedzenia pracowników. Audyt wewnętrzny obserwuje wykonywanie testów przez kierownictwo, koncentrując się na tym, czy: a) Wszyscy odpowiedni pracownicy są dostępni i zostali poinformowani w na czas. b) Urządzenia i zasoby zastępcze zaspokajają potrzeby jednostek biznesowych. c) Odpowiednie procedury tworzenia kopii zapasowych spełniły swoje zadanie. d) Testowanie objęło kluczowych partnerów biznesowych. e) Procesy biznesowe przywrócono w zakładanym czasie.
		2. Audyt wewnętrzny dokumentuje wyniki audytu.
	Działania po zakończeniu testowania	1. Zespół menadżerów BCM wykonuje analizę luk.
		2. Audyt wewnętrzny niezależnie wykonuje dokumentację oraz informuje o ewentualnych wnioskach z audytu.
		3. Należy przeanalizować wnioski BCM i obszary do poprawy oraz wprowadzić korekty; zespół menadżerów BCM omawia działania naprawcze i o wnioskach informuje odpowiednich interesariuszy. Takie dane mogą wspomóc rozwój BCM lub uaktualnienie planów.
		4. Konkluzje dotyczące programu testowania oraz tego, czy jest on odpowiedni dla wielkości, złożoności i profilu ryzyka organizacji należy udokumentować stosownie do treści planu.
		5. O wynikach testowania należy informować zarząd i/lub kierownictwo zarządzające.
	Szkolenie	1. Wszyscy pracownicy powinni być szkoleni i świadomi swoich obowiązków.
		2. Należy udokumentować szczegóły dotyczące szkoleń, takie jak treść, uczestnicy i termin.

Przykład 2:

Poniżej uzupełniono wybrane części oceny, by pokazać jej przykładową zawartość.

PRZYKŁADOWY PROGRAM PRAC BCM			
ELEMENT		STATUS	SPOSTRZEŻENIA DOTYCZĄCE OCENY
POWÓD, ZAKRES I CELE			
Zdefiniowanie programu	Czy program BCM jest udokumentowany, by definiować? • Zamiar, zakres i cele BCM. • Procedury BCM. • Zasoby, role i obowiązki BCM. • Pomiar i weryfikację BCM. • Stałe usprawnianie BCM.	Tak	Tak — ogólny zakres programu ustalony i udokumentowany.
	Czy w zakresie BCM mieści się cała działalność, w tym wszystkie procesy i operacje biznesowe, jak również powiązana z nimi infrastruktura i siła robocza, za które odpowiada firma?	Nie	Żadne elementy infrastruktury nie zostały wzięte pod uwagę.
PROCEDURY			
Ocena ryzyka Stworzona do określania scenariuszy zagrożeń (wiarygodnych zdarzeń), które mogą zakłócić działanie. Aby ukończyć niniejszą ocenę ryzyka BCM z powodzeniem, te osoby, które posiadają wiedzę na temat niebezpieczeństw zagrażających organizacji, środowisku, czy regionowi, powinny wziąć czynny udział. Wśród uczestników oceny ryzyka mogą znaleźć się pracownicy ochrony, infrastruktury, itp.	Czy przeprowadzono w organizacji ocenę ryzyka BCM?	PU (Potrzebne usprawnienie)	Potrzeba większej formalizacji i lepszej dokumentacji.
	Czy ocena ryzyka bierze pod uwagę następujące kategorie ryzyk: • Ryzyka naturalne. • Niepokoje społeczne/ludzie. • Czynniki ludzkie/IT. • Operacyjne.	PU	Pod uwagę należy wziąć zdarzenia regionalne.
Należy dokonać lokalnej oceny ryzyka BCM, a jej wyniki udostępnić odpowiednim najemcom obiektów/lokalizacji.	Czy określono strategię ograniczania ryzyka?		
	Czy ograniczono ryzyka?		
	Czy dana ocena ryzyka BCM (np. scenariusze postępowania w przypadku klęsk) została uzgodniona z pozostałymi organizacjami w regionie?		

Międzynarodowe Ramowe Praktyki Zawodowe (IPPF) – Praktyczny przewodnik Zarządzanie ciągłością działania

PRZYKŁADOWY PROGRAM PRAC BCM			
ELEMENT		STATUS	SPOSTRZEŻENIA DOTYCZĄCE OCENY
Analiza BIA Określa krytyczne procesy biznesowe, które należy przywrócić po wystąpieniu zdarzenia kryzysowego. Po dokonaniu analizy BIA należy określić rozwiązania odtworzeniowe potrzebne, by wznowić krytyczne procesy biznesowe.	Czy w odniesieniu do organizacji (w tym do wszystkich zespołów biznesowych) przeprowadzono analizę BIA?		
	Czy określono krytyczne procesy biznesowe?		
	Czy zespół menadżerów zatwierdził listę krytycznych procesów biznesowych w trakcie analizy BIA oraz powiązanych z nimi proponowanych rozwiązań odtworzeniowych?		
Rozwiązania odtworzeniowe Opracowywane są rozwiązania odtworzeniowe oraz lista zasobów potrzebnych do wspierania działań organizacji i/lub zespołu w zakresie zarządzania kryzysowego (proces odtworzeniowy).	Czy dla każdego krytycznego procesu określono wymagania dotyczące rozwiązań odtworzeniowych i zasobów?		
	Czy wszystkie zespoły udokumentowały zasoby wymagane do odtworzenia krytycznych procesów biznesowych?		
	Czy oceniono wymagania IT?		
Pisemne plany	Czy przygotowano pisemną wersję BCP zawierającą wszystkie zespoły biznesowe, krytyczne procesy biznesowe oraz organizacyjne CMP?		
Umowy o poziomie świadczonych usług (SLA), protokół ustaleń (MOU) i umowy	Czy ustanowiono umowy SLA i/lub MOU dotyczące: • Przestrzeni biurowej (z zarządem obiektów)? • IT/komunikacji (z dostawcą usług IT)? • Przywracania danych (z dostawcą usług IT)? • Inne umowy ze stronami trzecimi?		
	Czy podjęto działanie, by chronić interesy firmy, gdy umowy ze stronami trzecimi zawierają klauzulę „siły wyższej”?		
Ujednolicenie	Czy bierzesz udział w planowaniu skoordynowanym z innymi najemcami, innymi obiektami?		
	Czy Twoja organizacja opracowała dla wszystkich pracowników plan komunikacji awaryjnej obejmujący księgowość?		
	Czy BCP zostało dostosowane do zarządzania i reagowania kryzysowego?		

PRZYKŁADOWY PROGRAM PRAC BCM			
ELEMENT		STATUS	SPOSTRZEŻENIA DOTYCZĄCE OCENY
Szkolenie i ćwiczenia	Czy zarządzający BCM i menadżer BCM zostali przeszkoleni?		
	Czy koordynator BC został przeszkolony?		
	Czy wszyscy członkowie zespołu BCM odbyli szkolenie dotyczące ich ról i obowiązków?		
	Czy główne zadania BCM wykonywane są raz w roku, czy częściej? • Ćwiczenie procedury powiadamiania. • Ćwiczenie teoretyczne. • Ćwiczenie funkcjonalne. • Ćwiczenie w pełnym zakresie.		
ZASOBY, ROLA I OBOWIĄZKI			
Pracownicy wspomagający BCM	Czy sprawdzono, czy personel zastępczy, który będzie wykonywać zadania krytyczne posiada odpowiednie możliwości (wiedzę, dostęp, itp.), by pełnić taką rolę?		
Zarządzający BCM Pełni rolę orędownika BCM w organizacji (w tym współpracownika zespołu kierownictwa), wspierając tworzenie i wdrażanie planów BCM, poprzez efektywną koordynację funduszy, personelu oraz analizy planów biznesowych i ryzyk dotyczących danej organizacji.	Czy zespół zarządzający w danej organizacji wskazał zarządzającego BCM?		
	Czy zarządzający BCM ma dostęp do zespołu zarządzającego?		
	Czy fundusze, personel i zasoby są odpowiednie?		
	Czy BCM zostało skoordynowane z innymi procesami organizacyjnymi i połączone z planem biznesowym organizacji?		
Menadżer BCM	Czy wyznaczono menadżera BCM dla całej organizacji?		
	Czy menadżer BCM koordynuje i kieruje wdrażaniem BCM?		
	Czy menadżer BCM zapewnia dostępność wielofunkcyjnych zasobów oraz ich odpowiednie wykorzystanie?		
	Czy menadżer BCM zapewnia skuteczność i efektywność zarządzania kryzysowego, poprzez wycenianie, weryfikowanie i poddawanie go okresowemu przeglądowi celem wskazania możliwości ulepszeń?		

PRZYKŁADOWY PROGRAM PRAC BCM			
ELEMENT		STATUS	SPOSTRZEŻENIA DOTYCZĄCE OCENY
Koordinator BCM	Czy wyznaczono koordynatora BCM dla całej organizacji?		
	Czy koordynator BCM zarządza planowaniem ciągłości działania w organizacji, jednostce biznesowej (JB), regionalnej JB lub innych podjednostkach?		
	Czy, jeśli zajdzie taka potrzeba, koordynator BCM uczestniczy w działaniach koordynujących najemców i obiekty?		
POMIARY I WERYFIKACJA			
	Czy ustanowiono procesy pomiaru i weryfikacji, które co roku sprawdzają, czy wymogi BCM zostały spełnione w sposób zgodny z bieżącymi potrzebami biznesowymi?		
DOSKONALENIE			
	Czy potwierdzono wymagania IT, w tym wymogi IT dotyczące wspierania planowania relokacji, dostępu sieciowego lub zdalnego, danych lokalnych lub centralnych, itp.?		
	Czy procesy pomiaru i weryfikacji powiązane są z procesami ciągłego doskonalenia?		
	Czy śledzone są działania wymagane do usunięcia luk w BCM wskazanych podczas wykonywania BCM, w celu zapewnienia ukończenia zadania na czas?		
	Czy istnieje proces ponownej oceny programu BCM?		

Pomoce praktyczne II: Glosariusz kluczowych terminów

Plan ciągłości działania (BCP - Business Continuity Plan) – zdolność planowania ciągłości krytycznych procesów biznesowych, ochrony krytycznej infrastruktury oraz zapewnienia klientom obsługi i wsparcia w obliczu sytuacji kryzysowej, katastrofy, incydentu lub nagłego wypadku. Taki plan pozwala organizacji skutecznie odtworzyć procesy po wystąpieniu sytuacji kryzysowej oraz zarządzać ryzykami z nią związanymi. BCP jest częścią programu zarządzania kryzysowego.

Planowanie ciągłości działania i odtwarzania po awarii (BCRP - Business Continuity and Recovery Planning) – proaktywna metoda, dzięki której organizacje mogą określić środki do zarządzania kluczowymi ryzykami w organizacji wywołanymi przez sytuację kryzysową oraz do ich ograniczania.

Sytuacja kryzysowa – zdarzenie, które, przy nieodpowiedniej reakcji, może znacząco wpłynąć na zdolność organizacji do działania, utrzymania rentowności i zarządzania ryzykiem utraty reputacji. Są to zwykle katastrofy naturalne lub fizyczne, niepowodzenie krytycznych operacji i/lub łączności, zakłócenia w relacjach z partnerami biznesowymi oraz ryzyka technologiczne.

Program zarządzania kryzysowego (CMP - Crisis Management Program) – skonsolidowane portfolio czynności składające się z działań zapobiegawczych i reaktywnych wykonywanych przez organizację, w celu ograniczenia ryzyk związanych z sytuacją kryzysową lub zdarzeniem, i zarządzania nimi. CMP często zawiera plan ciągłości biznesowej oraz plan odtwarzania utraconych zasobów.

Katastrofa – nagłe, nieplanowane zdarzenie katastroficzne powodujące niedopuszczalne zniszczenia lub straty. Mogą to być zdarzenia, które zagrażają zdolności organizacji do zapewniania krytycznych funkcji, procesów lub usług. To przykład zdarzenia, w którym w ramach

ogólnego planu zarządzania kryzysowego często aktywowany jest plan ciągłości działania i/lub plan odtwarzania utraconych zasobów.

Nagły wypadek – nieplanowany i nieuchronny incydent lub sytuacja, które mogą spowodować uraz, utratę życia, zniszczenie własności lub ingerencję w normalne procesy biznesowe, ich utratę lub zakłócenie. Jeśli takie zdarzenia nie podlegają kontroli i zarządzaniu, mogą przerodzić się w sytuację kryzysową.

Incident – zdarzenie spoza standardów operacyjnych, które może mieć tymczasowy wpływ na działalność, a w niektórych przypadkach może prowadzić do nagłego wypadku lub katastrofy.

Analiza wpływów – proces analizy kluczowych funkcji operacyjnych lub danych krytycznych mający na uwadze zrozumienie potencjalnych wewnętrznych i zewnętrznych wpływów potencjalnej straty/zakłócenia. Analiza wpływów składa się z analizy BIA, która polega na identyfikacji krytycznych aktywów biznesowych, funkcji i zasobów, jak również na ocenie potencjalnych szkód lub strat dla organizacji wynikających z zakłócenia lub zmiany w środowisku biznesowym lub operacyjnym. Analiza BIA powinna wskazać: a) źródła szkód, zakłócenia lub straty, b) po jakim upływie czasu nastąpi zwiększenie potencjalnej szkody, zakłócenia lub straty, c) poziom usług lub zasoby potrzebne, by utrzymać zasadniczą działalność biznesową oraz d) czas, w jakim wszystkie krytyczne aktywa biznesowe, funkcje i zasoby powinny zostać przywrócone, by uniknąć stałej znaczącej straty dla organizacji.

Wskaźnik RPO (Recovery Point Objective – akceptowalny poziom utraty danych wyrażony w czasie) - punkt w czasie, do którego systemy i dane muszą zostać przywrócone po przestoju (np. koniec działania poprzedniego dnia). Wskaźniki RPO są często wykorzystywane jako podstawa opracowania strategii tworzenia kopii zapasowych oraz do określenia ilości danych, które być może trzeba będzie odtworzyć po przywróceniu systemów lub funkcji.

Wskaźnik przywracania działania w docelowym czasie (RTO - Recovery Time Objective) – okres, w którym systemy, aplikacje lub funkcje muszą zostać przywrócone po przestoju (zwykle jeden dzień roboczy). Wskaźniki RTO są często wykorzystywane jako podstawa opracowania strategii tworzenia kopii zapasowych oraz do określenia, czy strategię tę zostaną wdrożone w trakcie sytuacji kryzysowej. Terminem zwykle związanym ze wskaźnikiem RTO jest maksymalny dopuszczalny czas przestoju.

Ocena/Analiza ryzyka – proces identyfikacji ryzyk zagrażających organizacji, oceny funkcji krytycznych potrzebnych organizacji, by kontynuować działalność biznesową, zdefiniować kontrole mające na celu redukcję ryzyk organizacyjnych oraz oszacować koszty takich kontroli. Analiza ryzyka często składa się z oceny prawdopodobieństwa wystąpienia danego zdarzenia. Przykładem takiego zdarzenia jest sytuacja kryzysowa.

Pomoce praktyczne III: Standardy BCM oraz wytyczne

Standardy oraz wytyczne dotyczące BCM znajdują się w licznych źródłach. Należą do nich programy ramowe i modele dojrzałości określające rolę audytora wewnętrznego we wspieraniu cykli rozwojowych planu ciągłości działania (BCP) oraz planu zarządzania kryzysowego. Wiele z nich może służyć jako materiały edukacyjne dla pracowników audytu wewnętrznego i umożliwia dzielenie się wiedzą z kierownictwem, które zamierza rozpocząć, dostosować lub ocenić działania BCM. Od kwietnia 2013 roku do w/w źródeł należą:

- Międzynarodowe standardy profesjonalnej praktyki audytu wewnętrznego (Standardy) Instytutu Auditorów Wewnętrznych oraz podobne wytyczne (www.theiia.org), w tym:
 - o *Globalny Przewodnik Audytu Technologicznego 10: Zarządzanie ciągłością działania*. Przewodnik ten zawiera następujące elementy: 1) scenariusze

pospolitych katastrof, 2) rolę kadry zarządzającej podczas przerwy w działalności, 3) rozwiązania dotyczące odtwarzania utraconych zasobów, 4) ocenę i ograniczanie ryzyka, 5) przywracanie działalności oraz strategię ciągłości oraz 6) testowanie planu zarządzania kryzysowego.

- o 2010 GAIN Survey and Results-Crisis Management.
- o Audit Executive Center's 2011 Knowledge Alert-Three Crisis Management Imperatives for CAEs.
- ANSI/ASIS/BSI CM.01:2010, *Business Continuity Management Systems-Requirements With Guidance for Use* (2010). Współpraca między American National Standards Institute (ANSI), ASIS International oraz British Standards Institute (BSI) w celu opracowania programu ramowego kryteriów podlegających kontroli i towarzyszących im wytycznych, które można dopasować do potrzeb globalnych działań organizacji.
- Disaster Recovery Institute (www.drii.org), *Professional Practices for Business Continuity Planners* (2008). Szeroko stosowany program ramowy zawierający informacje na temat: 1) rozpoczęcia programu i zarządzania nim, 2) oceny i kontroli ryzyka, 3) analizy BIA, 4) strategii ciągłości działania, 5) reakcji i działań w sytuacjach wyjątkowych, 6) planów ciągłości działania, 7) programów informacyjnych i szkoleniowych, 8) audytu i utrzymania, 9) komunikacji oraz 10) koordynacji z agencjami zewnętrznymi.
- Federal Financial Institutions Examination Council (www.ffiec.gov), *Business Continuity Planning, IT Examination Handbook* (2008). Przewodnik składa się z następujących 7 elementów: 1) obowiązki zarządu i kadry zarządzającej wyższego stopnia, 2) proces planowania ciągłości działania, 3) analiza BIA, 4) ocena ryzyka, 5) zarządzanie ryzykiem, 6) monitorowanie i testowanie ryzyka oraz 7) pozostałe polityki, standardy i procesy.

- The Business Continuity Institute's (www.thebci.org) *Good Practice Guidelines* (2010). Wytyczne zawierają sześć elementów: 1) zarządzanie polityką i programem, 2) osadzenie zarządzania kryzysowego w kulturze organizacji, 3) zrozumienie działania organizacji, 4) wskazanie strategii zarządzania kryzysowego, 5) opracowanie i wdrożenie reakcji zarządzania kryzysowego oraz 6) wykonywanie, utrzymywanie i dokonywanie przeglądów.
 - Wytyczne ISO (International Organization for Standardization) (www.iso.org):
 - o ISO/*Publicly Available Specification (PAS) 22399, Societal Security-Guideline for Incident Preparedness and Operational Continuity Management* (2007). „Zawiera ogólne wytyczne dla organizacji (prywatnych, rządowych i pozarządowych) dotyczące opracowania własnych kryteriów gotowości na wypadek wystąpienia incydentu oraz ciągłości operacyjnej, a także opracowania odpowiedniego systemu zarządzania.”
 - o ISO/IEC 24762, *Guidelines for Information and Communications Technology Disaster Recovery Services* (2008). Zawiera wytyczne dotyczące zapewnienia usług związanych z odtwarzaniem utraconych zasobów technologii informatycznych i telekomunikacyjnych (ICT DR) w ramach BCM, znajdujące zastosowanie zarówno u własnych, jak i zewnętrznych dostawców usług ICT DR zapewniających infrastrukturę i usługi.
 - o ISO 27001, *Information Security Management* (2002). Pomaga organizacjom w opracowaniu zintegrowanego i kompleksowego systemu zarządzania bezpieczeństwem informacji, zawierającego najlepsze praktyki uznawane na całym świecie.
 - o ISO 22301, *Societal Security-Business Continuity Management Systems-Requirements*, standard, który zastąpił BS 25999. Określa ogólne wymagania systemu BCM obowiązujące we wszystkich organizacjach lub ich częściach.
 - British Standards Institute (www.bsigroup.com).
 - o PAS 200 (2011) doradza organizacjom w zakresie typów działań i zasobów, jakie powinny opracować i utrzymać, by umożliwić skuteczne wykrywanie, gotowość i działania w przypadku sytuacji kryzysowej. Niniejsza specyfikacja jest wspierana przez brytyjską Kancelarię Rządu, a specyfikacja dotycząca zarządzania kryzysowego została opracowana na drodze konsultacji z czołowymi brytyjskimi firmami i organizacjami publicznymi. Specyfikacja ta opisuje wymagania dotyczące zarządzania kryzysowego, jako dodatek do wytycznych zawartych w BS 25999: Business Continuity Management i ISO 27001.
 - o BS 25777: *Information and Communications Technology Continuity Management-Code of Practice* (2008). Zawiera zalecenia dotyczące zarządzania ciągłością technologii informacyjnych i telekomunikacyjnych w obrębie programu ramowego zarządzania ciągłością działania, zawartego w BS 25999-1.
- Organizacje wymienione powyżej prowadzą również działalność edukacyjną związaną z BCP i przyznają certyfikaty. Pozostałe organizacje oferujące takie szkolenia i certyfikaty to:
- Business Continuity Management Institute — www.CM-institute.org.
 - Business Continuity Planners Association — www.bcpa.org.
 - Business Resilience Certification Consortium International — www.brcci.org/index.htm.

Autorzy:

David Bentley, CIA
Brian Foster, CIA
Brian Peterson
Brian Reed, CIA
Erich Schumann, CIA, CRMA
Rita Thakkar, CIA
Benito Ybarra, CIA

Recenzent:

Steven E. Jameson, CIA, CCSA, CFSA, CRMA

Nadzór na projektem tłumaczenia:

Sebastian Burgemejster, CISA, CGAP, CCSA, CRMA

Kontrola jakości tłumaczenia:

Andrzej Brągiel, IIA Polska, Audytor Wewnętrzny
Sebastian Burgemejster, CISA, CGAP, CCSA, CRMA

Tłumaczenie:

Anna Ratajczyk

Skład DTP:

Marcin Boguś

O Instytucie

Instytut Audytorów Wewnętrznych (IIA) założony został w 1941 roku. To międzynarodowe stowarzyszenie zawodowe z siedzibą w Altamonte Springs, Floryda, USA. IIA jest międzynarodową instytucją reprezentującą profesję audytu wewnętrznego, uznanym autorytetem i liderem, głównym orędownikiem i edukatorem zasad.

O Instytucie IIA Polska

IIA jest reprezentowany w Polsce przez Instytut Audytorów Wewnętrznych IIA Polska. Instytut Audytorów Wewnętrznych IIA Polska jest stowarzyszeniem osób fizycznych, zarejestrowanym w Krajowym Rejestrze Sądowym 9 maja 2002 r. oraz uznanym przez światową organizację IIA w dniu 27 czerwca 2003 roku. Do Instytutu Audytorów Wewnętrznych IIA Polska należy aktualnie ponad 1500 osób z całego kraju. Instytut nie prowadzi działalności gospodarczej i opiera się na aktywności społecznej członków i wolontariuszy realizujących cele Instytutu.

O przewodnikach praktycznych

Przewodniki praktyczne zawierają szczegółowe wytyczne dotyczące przeprowadzania czynności audytu wewnętrznego. Szczegółowo opisują procesy

i procedury, takie jak narzędzia i metody, programy oraz podejścia krok po kroku, jak również przykładowe wyniki. Praktyczne przewodniki stanowią część Międzynarodowych Ramowych Praktyk Zawodowych (IPPF) IIA. W ramach kategorii „Szczególnie zalecane” zgodność nie jest obowiązkowa, ale zalecana. Wytyczne są zatwierdzane przez IIA poprzez formalne przeglądy i procesy zatwierdzania. Więcej materiałów na temat wytycznych IIA znajduje się na stronie <https://globaliia.org/standards-guidance>.

Zastrzeżenia

IIA publikuje niniejszy dokument w celach informacyjnych i edukacyjnych. Niniejszy materiał nie zapewnia ostatecznych odpowiedzi na specyficzne indywidualne okoliczności i jako taki powinien być wykorzystywany jedynie jako przewodnik. W odniesieniu do konkretnych sytuacji, IIA zaleca konsultacje z niezależnym ekspertem. IIA nie bierze odpowiedzialności za wyłączenie powoływanie się na niniejszy przewodnik.

Majątkowe prawa autorskie

Majątkowe prawa autorskie © 2014 Instytut Audytorów Wewnętrznych. Aby uzyskać zgodę na przetwarzanie, należy skontaktować się z IIA pod adresem guidance@theiia.org.



**The Institute of
Internal Auditors**

Global

GLOBAL HEADQUARTERS

247 Maitland Ave.

Altamonte Springs, FL 32701 USA

T: +1-407-937-1111

F: +1-407-937-1101

W: www.globaliia.org