Ten przykładowy szablon został zaprojektowany, aby pomóc użytkownikowi w przeprowadzeniu analizy wpływu na działalność (ang. Business Impact Analysis - BIA) w przypadku zakłócenia w systemie informatycznym. Szablon ma jedynie charakter przewodnika i może nie mieć jednakowego zastosowania do wszystkich systemów. Aby jak najlepiej dostosować się do konkretnego systemu, użytkownik może zmodyfikować ten szablon lub podejść do BIA zgodnie z ogólnymi wymaganiami,. W szablonie wyrazy kursywą służą wyłącznie jako wskazówki i powinny zostać usunięte z ostatecznej wersji. Tekst zwykły (nie kursywą) jest obligatoryjny.

1. Przegląd

Niniejsza analiza wpływu na działalność (BIA) została opracowana jako część procesu planowania awaryjnego dla *{nazwa systemu} {akronim systemu}*. Analizę przygotowano w dniu *{wstaw datę zakończenia BIA}*.

1.1 Cel

Celem BIA jest identyfikacja i uszeregowanie pod względem ważności elementów systemu poprzez skorelowanie ich z procesami biznesowymi obsługiwanymi przez system oraz wykorzystanie tych informacji do scharakteryzowania wpływu na proces (y), jeśli system byłby niedostępny.

BIA składa się z następujących trzech kroków:

1. **Określenia procesów biznesowych i krytyczności ich odzyskiwania**. Procesy biznesowe obsługiwane przez system są identyfikowane, a wpływ zakłócenia pracy systemu na te procesy jest określany wraz ze skutkami awarii i szacowanym czasem przestoju. Przestoje powinny odzwierciedlać maksimum, które organizacja może tolerować przy jednoczesnym utrzymaniu celu działania.
2. **Identyfikacji wymagań dotyczących zasobów**. Realistyczne działania naprawcze wymagają dogłębnej oceny zasobów wymaganych do jak najszybszego wznowienia procesów biznesowych. Przykłady zasobów, które należy zidentyfikować, obejmują obiekty, personel, sprzęt, oprogramowanie, pliki danych, inne komponenty systemu i niezbędne dane.
3. **Określenia priorytetów odzyskiwania zasobów systemowych**. W oparciu o wyniki poprzednich działań, zasoby systemowe można wyraźniej powiązać z krytycznymi procesami procesów biznesowych. Można ustalić poziomy priorytetów dla sekwencjonowania działań mających na celu odzyskanie zasobów.

Niniejszy dokument służy do zbudowania dla {*nazwa systemu*} Planu Awaryjnego dla Systemu Informatycznego (*ang. Information System Contingency Plan – ISCP*) i stanowi

kluczowy element ISCP. Może być również wykorzystywany do wspierania opracowywania innych planów awaryjnych związanych z systemem, w tym między innymi planu odzyskiwania po awarii (*ang. Disaster Recovery Plan - DRP*) lub planu reagowania na incydenty cyberbezpieczeństwa (*ang. Cyber Incident Response Plan - CIRP*).

2. Opis systemu

Podaj ogólny opis architektury systemu i jego funkcjonalności. Wskaż środowisko operacyjne, lokalizację fizyczną, ogólną lokalizację użytkowników oraz partnerstwa z zewnętrznymi organizacjami / systemami. Dołącz informacje dotyczące wszelkich innych zagadnień technicznych, które są ważne dla celów odzyskiwania, takich jak procedury tworzenia kopii zapasowych. Podaj schemat architektury, w tym wejścia i wyjścia oraz połączenia telekomunikacyjne.

Uwaga: informacje dla tej sekcji powinny być dostępne z Planu Bezpieczeństwa Systemu (System Security Plan – SSP) i można je skopiować z SSP lub odnieść się do odpowiedniej sekcji SSP i dołączyć najnowszą wersję SSP do tego planu awaryjnego.

3. Gromadzenie danych na potrzeby BIA

Gromadzenie danych można przeprowadzić poprzez wywiady indywidualne / grupowe, warsztaty, e-maile, kwestionariusze lub dowolną ich kombinację.

3.1 Określenie krytyczność procesu i systemu

Krok pierwszy procesu BIA - Praca z danymi wejściowymi uzyskanymi od użytkowników, kierowników, właścicieli procesów biznesowych oraz innych wewnętrznych lub zewnętrznych punktów kontaktowych (*ang. Point of Contact - PoC*), identyfikacja konkretnych procesów biznesowych, które zależą od systemu informatycznego lub go wspierają.

Proces Biznesowy	**Opis**
Opłata faktury od dostawcy	*Proces obciążania konta, wystawienia czeku lub płatności elektronicznej i potwierdzania odbioru*

Jeśli krytyczność procesów biznesowych nie została ustalona poza BIA, poniższe podrozdziały pomogą ustalić krytyczność procesów biznesowych, które zależą od wsparcia systemu informatycznego.

3.1.1 Zidentyfikuj wpływ awarii i szacowany czas przestoju

W tej sekcji zidentyfikowano i scharakteryzowano rodzaje kategorii wpływu, które może spowodować zakłócenie systemu, oprócz tych określonych przez poziom wpływu NSC 199, a także szacowany czas przestoju, który organizacja może tolerować dla danego procesu. Należy utworzyć kategorie skutków i przypisać wartości do tych kategorii w celu zmierzenia poziomu lub rodzaju wpływu, jaki może spowodować zakłócenie. Podano przykład kosztu jako kategorii wpływu. Organizacje mogą rozważyć inne kategorie, takie jak wyrządzenie szkody jednostkom i zdolność do osiągania celu działania. Szablon powinien zostać zmieniony, tak aby odzwierciedlić to, co jest odpowiednie dla danej organizacji.

Skutki awarii

Kategorie i wartości oddziaływania powinny być tworzone w celu scharakteryzowania poziomów dotkliwości dla organizacji, które wynikałyby dla tej konkretnej kategorii wpływu, gdyby nie można było wykonać procesu biznesowego. Te kategorie wpływu i ich wartości są próbkami i powinny zostać zmienione w celu odzwierciedlenia tego, co jest odpowiednie dla danej organizacji.

Następujące kategorie wpływu reprezentują ważne obszary, które należy rozważyć w przypadku zakłócenia.

Kategoria wpływu: *{wstaw nazwę kategorii}*

Wartości wpływu do oceny wpływu na kategorię:

- Poważny = *{wstaw wartość}*
- Umiarkowany = *{wstaw wartość}*
- Minimalny = *{wstaw wartość}*

Przykładowa kategoria wpływu: koszt

Poważny – koszty związane z incydentem są wyższe niż 1 milion PLN;

Umiarkowany – koszty związane z incydentem są od 550 tys. do 1mln. PLN;

Minimalny – koszty związane z incydentem są poniżej 550 tys. PLN

Poniższa tabela podsumowuje wpływ na każdy proces biznesowy, jeśli *{nazwa systemu}* byłby niedostępny, w oparciu o następujące kryteria:

Nazwa procesu	Kategoria wpływu				
	{wstaw}	*{wstaw}*	*{wstaw}*	*{wstaw}*	Wpływ*)
Opłacanie faktur dostawców					

*) – max. spośród wszystkich kategorii wpływu

Szacowanie czasu przestoju

Współpracując bezpośrednio z właścicielami procesów biznesowych, pracownikami komórek organizacyjnych, menedżerami i innymi zainteresowanymi stronami, oszacuj czynniki czasu przestoju, które należy uwzględnić w wyniku zdarzenia zakłócającego.

- **Maksymalny dopuszczalny czas przestoju (*ang. Maximum Torelable Downtime - MTD*)**. MTD reprezentuje całkowitą ilość czasu, którą menedżerowie są gotowi zaakceptować na przerwanie lub zakłócenie procesu biznesowego i obejmuje wszystkie aspekty dotyczące wpływu. Określenie MTD jest ważne, ponieważ może pozostawić planistom ciągłości nieprecyzyjny kierunek w sprawie (1) wyboru odpowiedniej metody odzyskiwania oraz (2) szczegółów, które będą wymagane przy opracowywaniu procedur odzyskiwania, w tym ich zakresu i zawartości.
- **Docelowy czas odzyskiwania (*ang. Recovery Time Objective - RTO*)**. RTO określa maksymalny czas, przez który zasób systemowy może pozostać niedostępny, zanim będzie miał nieakceptowalny wpływ na inne zasoby systemowe, obsługiwane procesy biznesowe i MTD. Określenie RTO jest ważne przy wyborze odpowiednich technologii, które najlepiej nadają się do spełnienia MTD.
- **Docelowy punkt odzyskiwania (*ang. Recovery Point Objective - RPO*)**. RPO reprezentuje moment czasu przed zakłóceniem lub awarią systemu, do którego można po awarii odzyskać dane procesu biznesowego (biorąc pod uwagę najnowszą kopię zapasową danych).

Poniższa tabela identyfikuje MTD, RTO i RPO (o ile ma zastosowanie) dla procesów biznesowych wspieranych przez *{nazwa systemu}.*

Oczekuje się, że wartości MTD i RPO będą ściśle zdefiniowanymi ramami czasowymi, określonymi w przyrostach godzinowych (np. 8 godzin, 36 godzin, 72 godziny itp.).

Nazwa procesu	**MTD**	**RTO**	**RPO**
Opłata za faktury dostawców	72 godz.	48 godz.	12 godz. (ostatnia kopia zapasowa)

Dołącz opis czynników wpływających na wymienione w powyższej tabeli parametry MTD, RTO i RPO (np. obciążenie pracą, miary wydajności, itp.)

Dołącz opis wszelkich alternatywnych środków (przetwarzanie wtórne lub ręczne) w celu odzyskania możliwości realizacji procesów biznesowych, które wspiera system. Jeśli środki te nie istnieją, to należy opisać.

3.2 Identyfikacja wymagań dotyczących zasobów

W poniższej tabeli wymieniono zasoby, które składają się na *{nazwa systemu}*, w tym sprzęt, oprogramowanie i inne zasoby, takie jak pliki danych.

Zasób systemowy / komponent	Platforma / system operacyjny / wersja (jeśli dotyczy)	Opis
Web Server 1	*Optiplex GX280*	*Web Site Host*

Zakłada się, że wszystkie zidentyfikowane zasoby wspierają procesy biznesowe określone w sekcji 3.1, chyba że zaznaczono inaczej.

Uwaga: informacje zawarte w tej sekcji powinny być dostępne z Planu Bezpieczeństwa Systemu (SSP) i można je skopiować z SSP lub odnieść się do odpowiedniej sekcji SSP i dołączyć najnowszą wersję SSP do tego planu awaryjnego.

3.3 Określanie priorytetów odzyskiwania zasobów systemowych

W poniższej tabeli wymieniono kolejność odzyskiwania zasobów *{nazwa systemu}*. Tabela określa również oczekiwany czas na odzyskanie zasobu po zakłóceniu w „najgorszym przypadku” (całkowita przebudowa / naprawa lub wymiana).

- **Docelowy czas odzyskiwania (RTO)** - RTO określa maksymalny czas, przez który zasób systemowy może pozostać niedostępny, zanim będzie miał nieakceptowalny wpływ na inne zasoby systemowe, obsługiwane procesy biznesowe i MTD. Określenie RTO dla poszczególnych zasobów systemu informatycznego jest ważne przy wyborze odpowiednich technologii, które najlepiej nadają się do spełnienia MTD.

Nazwa zasobu	Zasób / komponent systemu	Docelowy czas odzyskiwania (RTO)
Web Server 1	*Optiplex GX280*	*24 godz. na naprawę lub wymianę*

Zasobem systemowym może być oprogramowanie, pliki danych, serwery lub inny sprzęt i należy je identyfikować indywidualnie lub jako grupę logiczną.

Zidentyfikuj wszelkie alternatywne strategie, które spełniają oczekiwane RTO. Obejmuje to tworzenie kopii zapasowych lub zapasowego sprzętu i umowy wsparcia technicznego od dostawcy.