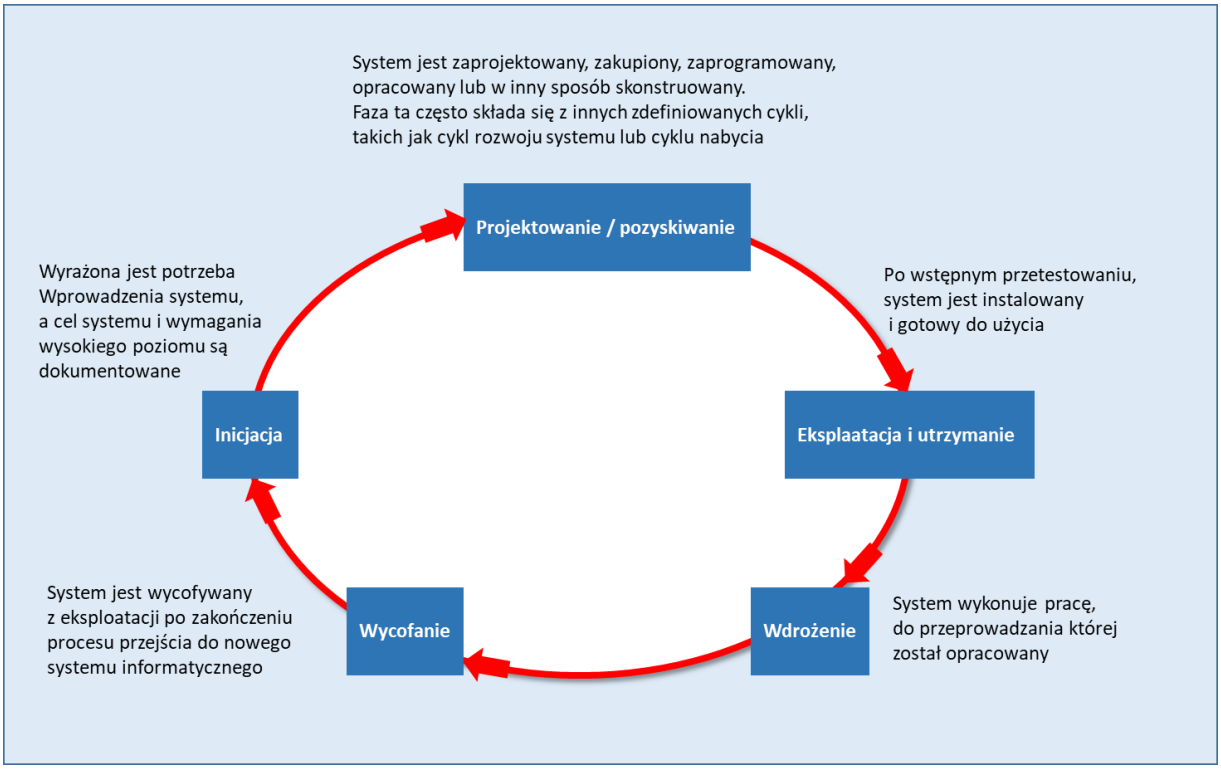
PLANOWANIE AWARYJNE A CYKL ŻYCIA SYSTEMU (SDLC)

Cykl życia systemu (*ang. system development life cycle - SDLC*) odnosi się do pełnego zakresu działań prowadzonych przez właścicieli systemów informatycznych związanych z systemem, z wyartykułowaniem potrzeby posiadania określonego systemu – inicjacją, projektowaniem / pozyskaniem systemu, jego wdrażaniem, eksploatacją i wycofaniem z użytkowania. Cykl życia systemu przedstawiony jest na rysunku F-1. Planowanie awaryjne wiąże się z działaniami występującymi głównie na etapie eksploatacji, jednak uwzględnienie strategii awaryjnych powinno mieć miejsce na wszystkich etapach cyklu życia systemu, co pozwala właścicielowi zbudować warstwową ochronę przed zagrożeniami i pomaga wdrożyć skuteczne strategie odzyskiwania na wczesnym etapie rozwoju systemu. Takie podejście zmniejsza ogólne koszty planowania awaryjnego, zwiększa możliwości awaryjne i zmniejsza wpływ na operacje systemu po wdrożeniu planu awaryjnego. W tej części przedstawiono popularne sposoby włączania strategii awaryjnych w całym SDLC. Podsumowanie okresów realizacji zabezpieczeń CP w SDLC znajduje się w Tabeli F-1. Szczegółowy opis działań i strategii awaryjnych znajduje się w rozdziale 5 - Uwagi techniczne dotyczące planowania awaryjnego.



Rysunek F - 1 Cykl życia systemu

Faza inicjacji. Przy opracowywaniu nowego systemu informatycznego należy wziąć pod uwagę wymagania dotyczące planowania awaryjnego. Podczas inicjacji powinna zostać uwzględniona potrzeba planowania awaryjnego, ponieważ wymagania systemu informatycznego są identyfikowane i dopasowywane do powiązanych funkcji operacyjnych, przeprowadzana jest ocena ryzyka w celu zrozumienia, przed czym system będzie potrzebował ochrony oraz ustala się cele dotyczące poufności, integralności i dostępności. Wysokie wymagania dotyczące dostępności systemu informatycznego mogą wskazywać, że w projekcie systemu powinny być wbudowane nadmiarowe kopie zapasowe w czasie rzeczywistym w alternatywnej lokalizacji i funkcje przełączania awaryjnego. Podobnie, jeśli system ma być aplikacją wirtualną, projekt może wymagać dodatkowych funkcji, takich jak zdalna diagnostyka lub możliwości samoistnego naprawiania się.

Podczas fazy inicjacji należy ocenić procesy biznesowe obsługiwane przez nowy system informatyczny i określić wymagania użytkowników dotyczące czasu odzyskiwania.

Zabezpieczenia planowania awaryjnego na tym etapie obejmują:

- CP-1: Polityka i procedury;
- CP-6: Zapasowe miejsce przechowywania kopii;
- CP-7: Zapasowe miejsce przetwarzania;
- CP-8: Usługi telekomunikacyjne;
- CP-9: Kopia zapasowa;
- CP-11 Alternatywne protokoły komunikacji;
- CP-12 Tryb bezpieczny;
- CP-13 Alternatywne mechanizmy bezpieczeństwa.

Faza projektowania / pozyskania. Gdy początkowe koncepcje ewoluują w projektowanie systemu informatycznego, można określić konkretne rozwiązania awaryjne. Podobnie jak w fazie inicjacji, względy techniczne planowania awaryjnego na tym etapie powinny odzwierciedlać wymagania systemowe i operacyjne. Projekt powinien uwzględniać

redundancję i niezawodność bezpośrednio w architekturze systemu, tak, aby zoptymalizować niezawodność, łatwość konserwacji i dostępność na późniejszym etapie eksploatacji. Uwzględniając strategię odzyskiwania podczas wstępnego projektowania, następuje zmniejszenie kosztów, a problemy związane z modernizacją lub modyfikacją systemu podczas fazy eksploatacji są zminimalizowane. Uwzględnienie tej tematyki na etapie projektowania / przejęcia zapewnia, że strategie planowania awaryjnego są odpowiednio uwzględniane w strategii odzyskiwania. Jeśli w ramach nowego systemu informatycznego hostowanych jest wiele aplikacji, należy ustalić sekwencję priorytetów odzyskiwania dla każdej z tych aplikacji, aby pomóc w wyborze odpowiedniej strategii odzyskiwania i sekwencji odzyskiwania przy wdrażaniu planu awaryjnego. Przykładami środków awaryjnych, które należy wziąć pod uwagę na tym etapie, są redundantne ścieżki komunikacyjne, eliminacja pojedynczych punktów awarii, zwiększona odporność na awarie komponentów i interfejsów sieciowych, systemy zarządzania energią z odpowiednio dobranymi źródłami zasilania rezerwowego, równoważenie obciążenia oraz dublowanie i replikacja danych, aby zapewnić wysoką dostępność systemu. Jeśli w ramach strategii wybrano dla celów odzyskiwania sytemu zapasowe miejsce przetwarzania, w tej fazie należy spełnić wymagania dotyczące tego miejsca.

Zabezpieczeniami planowania awaryjnego CP, które muszą być wzięte pod uwagę w tej fazie cyklu życia systemu są:

- CP-6: Zapasowe miejsce przechowywania kopii;
- CP-7: Zapasowe miejsce przetwarzania;
- CP-8: Usługi telekomunikacyjne;
- CP-9: Kopia zapasowa;
- CP-11 Alternatywne protokoły komunikacji;
- CP-12 Tryb bezpieczny;
- CP-13 Alternatywne mechanizmy bezpieczeństwa.

Faza wdrożenia. Wybrana strategia odzyskiwania jest teraz udokumentowana w formalnym planie awaryjnym systemu informacyjnego w koordynacji z zabiegiem testowaniem i oceny bezpieczeństwa (*ang. System Test and Evaluation - ST&E*). Ponieważ system przechodzi wstępne testy, należy również zastosować strategie awaryjne, aby rozwiązać wszelkie problemy związane z procedurami. Wyniki ćwiczeń mogą skłaniać do modyfikacji procedur odzyskiwania i planu awaryjnego.

Zabezpieczenia planowania awaryjnego, którymi należy się zająć na tym etapie, obejmują:

- CP-2: Plan ciągłości działania;
- CP-3: Szkolenia w zakresie planowania ciągłości działania;
- CP-4: Testowanie planu ciągłości działania.

Faza eksploatacji i utrzymania. Gdy system informatyczny już działa, użytkownicy, administratorzy i menedżerowie powinni utrzymywać program testów, szkoleń i ćwiczeń, który stale sprawdza procedury planu awaryjnego i strategię odzyskiwania. Ćwiczenia i testy powinny być przeprowadzane zgodnie z harmonogramem, tak, aby zapewnić, że procedury wcześniej opracowane będą nadal skuteczne. Należy rutynowo wykonywać pełne i przyrostowe kopie zapasowe oraz przechowywać je poza siedzibą, dokonywać rotacji nośników i okresowo sprawdzać ich poprawność. Plan awaryjny powinien być aktualizowany, tak, aby odzwierciedlał zmiany w procedurach wprowadzane na podstawie wniosków wyciągniętych z testów, ćwiczeń i faktycznych zakłóceń. Kiedy system informatyczny przechodzi modernizacje lub inne modyfikacje, takie jak zmiany w zewnętrznych interfejsach, modyfikacje te powinny znaleźć odzwierciedlenie w planie awaryjnym. Aby utrzymać aktualność i skuteczność planu, koordynowanie i dokumentowanie zmian w planie powinno odbywać się w odpowiednim czasie.

W tej fazie zabezpieczenia planowania awaryjnego obejmują:

- CP-2: Plan ciągłości działania;
- CP-3: Szkolenia w zakresie planowania ciągłości działania;
- CP-4: Testowanie planu ciągłości działania;

- CP-9: Kopia zapasowa;
- CP-10: Odzyskiwanie i odtwarzanie systemu.

Faza wycofania. Kwestie awaryjne nie powinny być zaniedbywane również w fazie wycofania i zastępowania systemu przez inny system. Dopóki nowy system nie będzie w pełni operacyjny i nie zostanie w pełni przetestowany (w tym pod względem możliwości awaryjnych), ISCP oryginalnego systemu należy utrzymywać w stanie gotowości do wdrożenia. Zastępowane systemy informatyczne mogą zapewnić cenne możliwości, jako system redundantny na wypadek utraty lub awarii nowego systemu. W niektórych przypadkach część sprzętu (np. dyski twarde, zasilacze, układy pamięci lub karty sieciowe) z wymienionego sprzętu można wykorzystać, jako części zamienne w nowym systemie. Ponadto, starsze systemy informatyczne mogą być wykorzystywane, jako systemy testowe dla nowych aplikacji, umożliwiając identyfikację i naprawę potencjalnych wad systemu w środowisku nieprodukcyjnym.

W tej fazie zabezpieczenia planowania awaryjnego obejmują:

- CP-2 Plan ciągłości działania;
- CP-9: Kopia zapasowa;
- CP-10: Odzyskiwanie i odtwarzanie systemu;
- CP-11 Alternatywne protokoły komunikacji;
- CP-12 Tryb bezpieczny;
- CP-13 Alternatywne mechanizmy bezpieczeństwa.

Tabela F-1: Implementacja zabezpieczeń CP w SDLC

Identyfikator zabezpieczenia	Nazwa zabezpieczenia	Inicjowanie	Projektowanie lub pozyskanie	Wdrażanie	Eksploatacja	Wycofanie
CP-1	Zasady i procedury planowania awaryjnego	X				
CP-2	Plan awaryjny			X	X	X
CP-3	Szkolenia w zakresie planowania awaryjnego			X	X	
CP-4	Testowanie planu awaryjnego			X	X	
CP-5	Uaktualnianie planu awaryjnego (wycofane)	-----	-----	-----	-----	-----
CP-6	Zapasowe miejsce składowania danych	X	X			
CP-7	Zapasowe miejsce przetwarzania	X	X			
CP-8	Usługi telekomunikacyjne	X	X			
CP-9	Kopia zapasowa systemu informatycznego	X	X		X	X
CP-10	Odzyskiwanie i odtwarzanie systemu informatycznego				X	X
CP-11	Alternatywne protokoły komunikacji	X	X			X

Identyfikator zabezpieczenia	Nazwa zabezpieczenia	Inicjowanie	Projektowanie lub pozyskanie	Wdrażanie	Eksploatacja	Wycofanie
CP-12	Tryb bezpieczny	X	X			X
CP-13	Alternatywne mechanizmy bezpieczeństwa	X	X			X