| NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA | Narodowy Standard Cyberbezpieczeństwa | | |
|---|---|---|---|
| Nazwa standardu | Symbol | Wersja | Data wydania |
| **Poradnik Planowania Awaryjnego** | NSC 800-34 | 1.0 | 10/09/2021 |

# Poradnik Planowania Awaryjnego

**PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA**
**Warszawa 2021**

***Szanowni Państwo,***

Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów udostępnia do wykorzystania w Państwa działalności zestaw publikacji specjalnych. Stanowią one rekomendację w postaci Narodowych Standardów Cyberbezpieczeństwa, o których mowa w kierunku interwencji 6.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Mimo, że prezentowane standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST), to posiadają one mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, stosowane w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych.

Zaprezentowane publikacje stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę, jaka w tym zakresie stosowana jest w administracji federalnej USA.

Na prezentowany zestaw publikacji składają się następujące pozycje:[1]

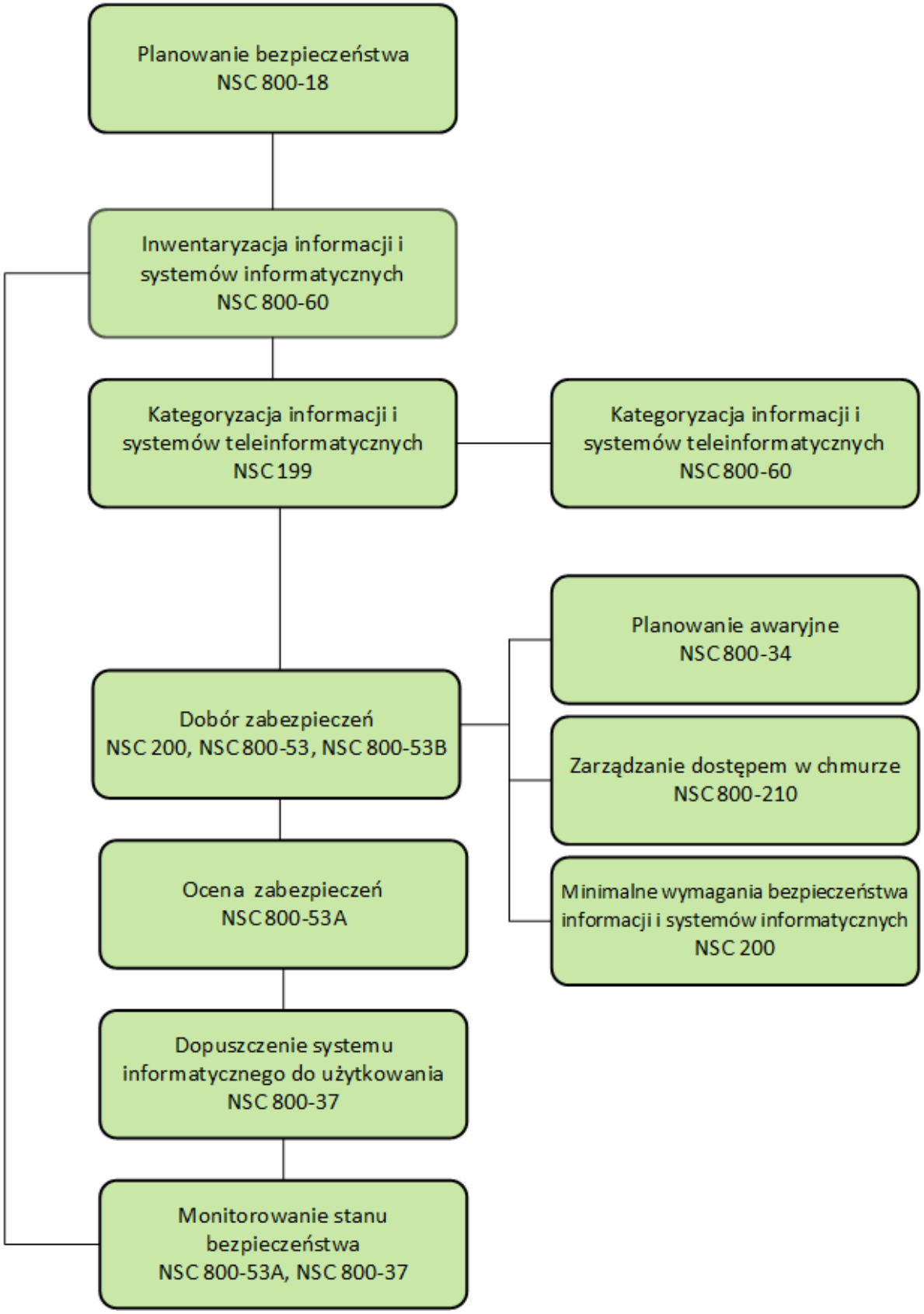
- NSC[2] 199, *Standardy kategoryzacji bezpieczeństwa* – na podstawie FIPS 199;
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych* – na podstawie FIPS 200;
- NSC 500-92, *Architektura referencyjna chmury obliczeniowej – rekomendacje* – na podstawie NIST SP 500-292;
- NSC 800-18, *Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych* – na podstawie NIST SP 800- 18;

[1] Wymienione są podstawowe dokumenty. Każdy z nich może się odwoływać w rozdziale *Referencje* do szeregu powiązanych publikacji, które składają się na całościowy proces osiągania cyberbezpieczeństwa.
[2] NSC – Narodowy Standard Cyberbezpieczeństwa.

- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* – na podstawie NIST SP 800-30;
- NSC 800-34, *Poradnik planowania awaryjnego* – na podstawie NIST SP 800-34;
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* – na podstawie NIST SP 800-37;
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53;
- NSC 800-53A, *Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny* – na podstawie NIST SP 800-53A;
- NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53B;
- NSC 800-60, *Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego* – na podstawie NIST SP 800-60;
- NSC 800-61, *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* – na podstawie NIST SP 800-61;
- NSC 800-210, *Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej* – na podstawie NIST SP 800-210.

Korzystając z tych publikacji można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem bazujący na publikacjach NIST wykorzystuje następujące dokumenty:


Planowanie bezpieczeństwa
NSC 800-18
Inwentaryzacja informacji i systemów informatycznych
NSC 800-60
Kategoryzacja informacji i systemów teleinformatycznych
NSC 199
Kategoryzacja informacji i systemów teleinformatycznych
NSC 800-60
Dobór zabezpieczeń
NSC 200, NSC 800-53, NSC 800-53B
Planowanie awaryjne
NSC 800-34
Zarządzanie dostępem w chmurze
NSC 800-210
Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych
NSC 200
Ocena zabezpieczeń
NSC 800-53A
Dopuszczenie systemu informatycznego do użytkowania
NSC 800-37
Monitorowanie stanu bezpieczeństwa
NSC 800-53A, NSC 800-37

**WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI**

National Institute of Standards and Technology (NIST) opracował wiele standardów i wytycznych w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością operacji organizacyjnych i majątku, osób fizycznych, innych organizacji i Państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych, a także dzięki jednolitemu podejściu, ułatwia wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznymi i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (np. ISO), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

Publikacje NIST, co do zasady, nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dozwolone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejście do zagadnień związanych z bezpieczeństwem informacji, systemów teleinformatycznych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie podmioty w opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Identyfikacja taka nie ma na celu nakłaniania do nich lub ich poparcia, nie ma też na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w tym obszarze.

W niniejszym Narodowym Standardzie Cyberbezpieczeństwa (NSC) mogą znajdować się odniesienia do innych publikacji opracowywanych obecnie przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa zgodnie z przypisanymi mu obowiązkami ustawowymi. Informacje zawarte w tej publikacji, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji, obowiązują aktualne wymagania, wytyczne i procedury, jeśli takie istnieją. W celach planistycznych i wprowadzania zmian, organizacje będą mogły uważnie śledzić rozwój tych nowych publikacji opracowywanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Niniejsza publikacja, ***Poradnik Planowania Awaryjnego***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-34, Rev. 1.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.***

# SPIS TREŚCI

# PODSUMOWANIE ZARZĄDCZE

Przewodnik planowania awaryjnego dla publicznych systemów informatycznych, zawiera instrukcje, zalecenia i uwagi w tym zakresie. Planowanie awaryjne dotyczy środków tymczasowych służących do odzyskiwania usług systemu informatycznego po zakłóceniu (*ang. Disruption*) ich funkcjonowania. Środki tymczasowe mogą obejmować przeniesienie systemów i operacji informatycznych do alternatywnego miejsca, odzyskanie funkcji systemu informatycznego przy użyciu alternatywnego sprzętu lub wykonanie funkcji systemu informacyjnego przy użyciu metod ręcznych. W przewodniku tym omówiono zalecenia dotyczące planowania awaryjnego dla trzech rodzajów platform oraz przedstawiono strategie i techniki wspólne dla wszystkich systemów:

- Systemy klient / serwer;
- Systemy telekomunikacyjne;
- Systemy klasy mainframe.

Niniejszy przewodnik określa następujący siedmiostopniowy proces planowania awaryjnego, który organizacja może wykorzystać w celu opracowania i utrzymania realnego programu planowania awaryjnego dla swoich systemów informatycznych. Te siedem kroków zaprojektowano tak, aby były zintegrowane z każdym etapem cyklu życia systemu.

1. Opracuj deklarację dotyczącą polityki planowania awaryjnego. Formalna polityka zapewnia autorytet i wytyczne niezbędne do opracowania skutecznego planu awaryjnego.
2. Przeprowadź analizę wpływu na działalność (*ang. business impact analysis - BIA*). BIA pomaga identyfikować systemy informatyczne i komponenty oraz nadawać im priorytety, mające kluczowe znaczenie dla wspierania misji / procesów biznesowych organizacji. Do przewodnika załączono szablon do opracowania BIA pomocny użytkownikowi w przeprowadzeniu analizy wpływu na działalność.

3. Zidentyfikuj środki zapobiegawcze. Środki podjęte w celu ograniczenia skutków zakłóceń w systemie mogą zwiększyć dostępność systemu i zmniejszyć ewentualne koszty cyklu życia.
4. Twórz strategie awaryjne. Dokładne strategie odzyskiwania zapewniają szybkie i skuteczne odzyskanie systemu po zakłóceniu.
5. Opracuj plan awaryjny systemu informatycznego. Plan awaryjny powinien zawierać szczegółowe wytyczne i procedury przywracania uszkodzonego systemu, zależnie od jego poziomu bezpieczeństwa i wymagań dotyczących odzyskiwania.
6. Zapewnij planowanie testów, szkoleń i ćwiczeń. Testowanie weryfikuje możliwości odzyskiwania, podczas gdy szkolenie przygotowuje personel do odzyskiwania podczas aktywacji planu, a wykonywanie planu identyfikuje luki w planowaniu; połączone działania poprawiają skuteczność planu i ogólną gotowość organizacji.
7. Zapewnij utrzymanie planu w aktualności. Plan powinien być żywym dokumentem, który jest regularnie aktualizowany, aby nadążał za zmianami w systemach teleinformatycznych i zmianami organizacyjnymi.

W niniejszym przewodniku przedstawiono trzy przykładowe formaty opracowywania planu awaryjnego systemu informatycznego charakteryzującego się niskim, umiarkowanym lub wysoki poziom oddziaływania zakłócenia. Każdy format definiuje trzy fazy określające działania, które należy podjąć po awarii systemu. Faza **Aktywacji / Powiadomienia** opisuje proces aktywacji planu na podstawie skutków awarii oraz powiadamiania personelu zaangażowanego w odzyskiwanie. Faza **Odzyskiwania** opisuje sugerowane działania zespołów odzyskiwania w celu przywrócenia działania systemu w alternatywnej lokalizacji lub korzystania z funkcji awaryjnych. Ostatnia faza, **Odtwarzanie** obejmuje działania mające na celu przetestowanie i sprawdzenie zdolności i funkcjonalności systemu oraz nakreśla działania, które można podjąć, aby przywrócić system do normalnych warunków działania i przygotować system na przyszłe awarie.

# ROZDZIAŁ 1 WSTĘP

Systemy informacyjne są istotnymi elementami w większości procesów biznesowych. Ponieważ zasoby systemu informacyjnego są tak istotne dla sukcesu organizacji, bardzo ważne jest, aby zidentyfikowane usługi świadczone przez te systemy mogły działać skutecznie bez nadmiernych zakłóceń. Planowanie awaryjne wspiera ten wymóg, ustanawiając dokładne plany, procedury i środki techniczne, które mogą umożliwić odzyskanie systemu po awarii usługi tak szybko i skutecznie, jak to możliwe. Planowanie awaryjne jest unikatowe dla każdego systemu, zapewniając środki zapobiegawcze, strategie odzyskiwania oraz aspekty techniczne odpowiednie do wymogów poufności, integralności i dostępności informacji w systemie oraz poziomu wpływu systemu na działalność organizacji.

Planowanie awaryjne systemu informacyjnego odnosi się do skoordynowanej strategii obejmującej plany, procedury i środki techniczne, które umożliwiają odzyskanie systemów informatycznych, operacji i danych po zakłóceniu. Planowanie awaryjne zazwyczaj obejmuje jedno lub więcej z następujących podejść do przywracania zakłóconych usług:

- Przywracanie systemów informatycznych przy użyciu alternatywnego sprzętu;
- Wykonywanie wybranych lub wszystkich procesów biznesowych, których dotyczy problem, przy użyciu alternatywnych metod przetwarzania (ręcznych), zazwyczaj akceptowalnych tylko w przypadku krótkotrwałych zakłóceń;
- Odzyskiwanie funkcjonowania systemów informatycznych w alternatywnej lokalizacji (zazwyczaj akceptowalnej tylko w przypadku długotrwałych zakłóceń lub tych, które fizycznie wpływają na obiekt);
- Wdrożenie odpowiednich zabezpieczeń planowania awaryjnego w oparciu o poziom wpływu systemu informatycznego na bezpieczeństwo.

Niniejszy dokument zawiera wytyczne dla osób odpowiedzialnych za przygotowanie i utrzymanie planów awaryjnych systemu informatycznego (*ang. information system contingency plans - ISCPs*). Dokument omawia podstawowe elementy i procesy planu

awaryjnego, uwypukla konkretne uwagi i sprawy związane z planowaniem awaryjnym odnoszącym się do różnych rodzajów platform systemów informatycznych oraz podaje przykłady, które pomogą czytelnikom w opracowaniu własnych ISCP.

## 1.1 CEL

Publikacja pomaga organizacjom w zrozumieniu celu, procesu i formatu rozwoju ISCP poprzez podanie praktycznych wytycznych odnoszących się do rzeczywistych sytuacji. Chociaż zasady te ustanawiają punkt odniesienia w celu zaspokojenia potrzeb większości organizacyjnych, uznaje się, że każda organizacja może mieć dodatkowe, specyficzne dla własnego środowiska operacyjnego. Niniejszy poradnik zawiera podstawowe informacje na temat powiązań między planowaniem awaryjnym systemu informacyjnego, a innymi rodzajami planów awaryjnych związanych z zarządzaniem bezpieczeństwem i zarządzaniem kryzysowym, odpornością organizacyjną i cyklem życia systemu (*ang. system development life cycle - SDLC*). Dokument zawiera wskazówki, które pomogą personelowi ocenić systemy i operacje informacyjne w celu ustalenia wymagań i priorytetów planowania awaryjnego. Zalecane zabezpieczenia (*ang. Security Controls*) są zgodne z wymaganiami NSC 800-53. Aby pomóc planistom w opracowaniu odpowiedniej strategii planowania awaryjnego uwzględniono poziomy wpływu i związane z tym środki zabezpieczeń mające zastosowanie do planowania awaryjnego. Chociaż informacje przedstawione w tym dokumencie są w dużej mierze niezależne od konkretnych platform sprzętowych, systemów operacyjnych i aplikacji, uwzględniono kwestie techniczne wspólne dla różnych platform systemów informatycznych.

## 1.2 ZAKRES

Dokument został opublikowany, jako zalecane wytyczne dla podmiotów publicznych, jednak może znaleźć zastosowanie w dowolnej organizacji. Aby pomóc personelowi odpowiedzialnemu za opracowanie planów awaryjnych, w niniejszym dokumencie omówiono popularne technologie, które można wykorzystać do wspierania zdolności do pracy w sytuacjach awaryjnych. Biorąc pod uwagę szeroki zakres projektów i konfiguracji systemów informatycznych, a także szybki rozwój i starzenie się produktów, omawiana problematyka nie jest wyczerpująca. Zamiast tego dokument opisuje praktyki technologiczne

mające na celu zwiększenie możliwości planowania awaryjnego systemu informatycznego organizacji. Wytyczne przedstawiają zasady planowania awaryjnego dla następujących wspólnych typów platform:

- Systemy klient / serwer;
- Systemy telekomunikacyjne;
- Systemy klasy mainframe.

Dokument określa zasady planowania dla wielu różnych incydentów, które mogą wpłynąć na działanie systemu informatycznego. Obejmują one od drobnych incydentów powodujących krótkotrwałe zakłócenia po katastrofy, które mają wpływ na normalne funkcjonowanie przez dłuższy okres. Ponieważ systemy informacyjne różnią się konstrukcją i przeznaczeniem, w niniejszym przewodniku nie omówiono konkretnych rodzajów incydentów i powiązanych z nimi środków łagodzących awarie. Zamiast tego przedstawiono określony proces identyfikacji wymagań planowania, niezbędnych do opracowania skutecznego planu awaryjnego dla dowolnego systemu informatycznego.

Niniejszy dokument nie dotyczy planowania systemu informatycznego na poziomie obiektu (zwanego zwykle planem odtworzenia po katastrofie – *ang. disaster recovery plan - DRP*) ani ciągłości misji organizacyjnej (powszechnie określanej, jako plan kontynuacji operacji (ang. *continuity of operations plan - COOP*), z wyjątkiem sytuacji, gdy wymagane jest przywrócenie systemów informatycznych i ich możliwości przetwarzania. Dokument ten nie dotyczy również ciągłości procesów misji / biznesowych. Chociaż systemy informacyjne zwykle obsługują procesy biznesowe, procesy te zależą również od wielu innych zasobów i możliwości niezwiązanych z systemami informatycznymi. Odzyskanie podstawowych funkcji biznesowych jest uwzględnione w planach COOP lub planach ciągłości działania. Plany te są częścią pakietu planów związanych z bezpieczeństwem i zarządzaniem kryzysowym, które zostały opisane w Podrozdziale 2.2. ISCP można przygotować w koordynacji z planowaniem odzyskiwania po awarii, planowaniem COOP lub planowaniem ciągłości działania, w stopniu, w jakim określony system jest niezbędny do zapewnienia zdolności wymaganej podczas któregokolwiek z tych zdarzeń / działań.

Informacje w tym przewodniku są zgodne z wytycznymi zawartymi w innych dokumentach, w tym z NSC 800-53. Proponowane wytyczne są również zgodne z obowiązującymi przepisami prawa w zakresie bezpieczeństwa systemów teleinformatycznych.

System informatyczny:

System informatyczny to określony zestaw zasobów zorganizowany w celu gromadzenia, przetwarzania, konserwacji, użytkowania, udostępniania, rozpowszechniania lub usuwania informacji.

Komponenty systemu informatycznego obejmują między innymi komputery mainframe, serwery, stacje robocze, komponenty sieciowe, systemy operacyjne, oprogramowanie systemowe i aplikacje. Komponenty sieciowe mogą obejmować na przykład takie urządzenia, jak zapory sieciowe, czujniki (lokalne lub zdalne), przełączniki, urządzenia ochronne, routery, bramy, punkty dostępu bezprzewodowego i zintegrowane rozwiązania urządzeń sieciowych. Serwery mogą obejmować na przykład serwery baz danych, serwery uwierzytelniania, pocztę elektroniczną i serwery WWW, serwery procy, serwery nazw domen i sieciowe serwery czasu. Komponenty systemu informacyjnego są albo kupowane „od ręki", albo są opracowane na zamówienie.

## 1.3 ODBIORCY

Dokument został stworzony dla menedżerów oraz osób odpowiedzialnych za systemy informatyczne lub bezpieczeństwo tych systemów. Wspomaga również personel zarządzający w sytuacjach kryzysowych, który koordynuje nieprzewidziane sytuacje na poziomie organizacji z działaniami wspierającymi planowanie awaryjne systemu informatycznego. Zalecenia przedstawione w tym dokumencie są odpowiednie dla systemów podmiotów publicznych, ale mogą być wykorzystywane przez organizacje prywatne i komercyjne, w tym systemy wykonawców. Do odbiorców dokumentu należą:

- Kierownicy odpowiedzialni za nadzorowanie operacji systemu informatycznego lub procesów biznesowych wspieranych przez systemy informatyczne;

- CIO[3] odpowiedzialni za systemy informacyjne organizacji;
- SAISO odpowiedzialni za rozwój i utrzymanie bezpieczeństwa systemów informatycznych na poziomie organizacyjnym;
- ISSO / ISSM oraz inny personel odpowiedzialny za opracowywanie, wdrażanie i utrzymywanie działań związanych z bezpieczeństwem systemu informatycznego;
- Inżynierowie systemów i architekci odpowiedzialni za projektowanie, wdrażanie lub modyfikowanie systemów informatycznych;
- Administratorzy systemu odpowiedzialni za utrzymanie codziennych operacji systemu informatycznego;
- Użytkownicy używający komputerów stacjonarnych i przenośnych do wykonywania przypisanych im zadań;
- Inni pracownicy odpowiedzialni za projektowanie, zarządzanie, obsługę, konserwację lub korzystanie z systemów informatycznych

[3] Patrz: Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa, NSC 7298.
Dotyczy to skrótów stosowanych w całym dokumencie.

## 1.4 STRUKTURA DOKUMENTU

Dokument ma na celu logiczne poprowadzenie czytelnika przez proces opracowywania planu awaryjnego. Proces ten obejmuje zaprojektowanie programu planowania awaryjnego, ocenę potrzeb organizacji w stosunku do opcji strategii awaryjnej na podstawie poziomów wpływu na system, zabezpieczeń i względów technicznych oraz udokumentowanie strategii awaryjnej w planie awaryjnym, przetestowanie planu i utrzymanie go. Powstały plan awaryjny służy jako „instrukcja użytkownika" do realizacji strategii w przypadku zakłócenia działania organizacji. Aby zapewnić lepsze zrozumienie, tam gdzie to możliwe, podano przykłady lub sytuacje hipotetyczne.

Pozostałe rozdziały tego dokumentu dotyczą następujących obszarów planowania awaryjnego:

- **Rozdział 2. Tło** zawiera podstawowe informacje o planowaniu awaryjnym, w tym o celach różnych planów związanych z zarządzaniem bezpieczeństwem i zarządzaniem sytuacjami kryzysowymi, ich relacjami z ISCP oraz o tym, jak plany te są zintegrowane z ogólną strategią odporności organizacji poprzez wdrożenie sześciu etapów Ramy zarządzania ryzykiem (*ang. Risk Management Framework - RMF*). Ponadto wyjaśniono również sposób, w jaki należy uwzględnić zabezpieczenia w zakresie planowania awaryjnego zgodnie z NSC 800-53 podczas procesu planowania awaryjnego.
- **Rozdział 3. Proces planowania awaryjnego dla systemu informatycznego**, wyszczególnia podstawowe zasady planowania niezbędne do opracowania skutecznej zdolności w opanowaniu awarii. Zasady przedstawione w tym rozdziale mają zastosowanie do wszystkich systemów informatycznych. W tym rozdziale przedstawiono wytyczne planowania awaryjnego dla wszystkich faz cyklu planowania, w tym analizy wpływu na działalność, wyboru lokalizacji alternatywnej i strategii odzyskiwania. W tym rozdziale omówiono także tworzenie zespołów planowania awaryjnego oraz role i obowiązki przypisywane personelowi podczas aktywacji planu.

- **Rozdział 4. Opracowanie planu awaryjnego systemu informatycznego**, opisuje działania niezbędne do udokumentowania strategii awaryjnej i opracowania ISCP. W tej części omówiono także utrzymanie, testowanie, szkolenie i wykonywanie planu awaryjnego.
- **Rozdział 5. Zagadnienia związane z planowaniem awaryjnym**, opisuje kwestie związane z planowaniem awaryjnym specyficzne dla trzech popularnych typów platform wymienionych w Podrozdziale 1.2 Zakres. Ten rozdział pomaga planistom awaryjnym zidentyfikować, wybrać i wdrożyć odpowiednie techniczne środki awaryjne dla ich systemów.

Dokument zawiera dziewięć załączników. Załącznik A zawiera trzy przykładowe szablony ISCP, uwzględniające poziom wpływu na działalność. Załącznik B przedstawia przykładowy szablon BIA. Załącznik C zawiera listę często zadawanych pytań na temat planowania awaryjnego systemu informatycznego. Problemy istotne z punktu widzenia planowania personelu są omówione w Załączniku D. Załącznik E zawiera podsumowanie zabezpieczeń planowania awaryjnego zgodnie z NSC 800-53 oraz ulepszeń tych zabezpieczeń. Załącznik F wyjaśnia integrację planowania awaryjnego z SDLC organizacji. Załączniki G i H zawierają odpowiednio słowniczek terminów i akronimów.

# ROZDZIAŁ 2 TŁO

Systemy informatyczne są podatne na różnego rodzaju zakłócenia, od łagodnych (np. krótkotrwała przerwa w zasilaniu, awaria dysku) do poważnych (np. zniszczenie urządzeń, pożar). Dużą podatność na wpływ zagrożenia można zminimalizować lub wyeliminować poprzez zabezpieczenia zarządcze, operacyjne lub techniczne w ramach działań organizacji, mające na celu uzyskanie odporności na takie zdarzenia, jednak całkowite wyeliminowanie wpływu wszystkich zagrożeń jest praktycznie niemożliwe. Planowanie awaryjne ma na celu zmniejszenie ryzyka niedostępności systemu i usług poprzez zapewnienie skutecznych i wydajnych rozwiązań zwiększających dostępność systemu.

W tym rozdziale omówiono sposoby, w jakie planowanie awaryjne systemu informatycznego wpisuje się w większe przedsięwzięcia związane z zarządzaniem ryzykiem, bezpieczeństwem i gotowością na wypadek awarii w organizacji (z których każdy jest kluczowym elementem w opracowywaniu programu odporności). Opisano również inne rodzaje planów gotowości na wypadek sytuacji nadzwyczajnych oraz ich relacje z planowaniem awaryjnym systemu informatycznego. Omówiono także, w jaki sposób integracja zasad planowania awaryjnego w całym SDLC promuje kompatybilność systemu i opłacalny sposób zwiększenia zdolności organizacji do szybkiego i skutecznego reagowania na zdarzenia zakłócające działanie systemów.

## 2.1 PLANOWANIE AWARYJNE I ODPORNOŚĆ NA ZAGROŻENIA

Organizacja musi mieć zdolność do wytworzenia odporności na różnego rodzaju zagrożenia i osiągnąć zdolność do podtrzymania swojej misji mimo zmian w środowisku. Zmiany te mogą być stopniowe, takie jak uwarunkowania gospodarcze lub zmiany celu działania organizacji lub nagłe, np. katastrofy. Zamiast tylko identyfikować i łagodzić wpływ zagrożenia, podatności i ryzyka, organizacje powinny pracować nad budowaniem odpornej infrastruktury, minimalizującej wpływ zakłóceń na podstawowe funkcje celu swojego działania.

Odporność to zdolność szybkiego dostosowywania się i odzyskiwania zdolności do funkcjonowania po zajściu znanych lub nieznanych zmian w środowisku. Odporność nie jest

procesem, ale raczej stanem końcowym. Celem odporności organizacji jest uzyskanie możliwości kontynuowania podstawowych funkcji biznesowych w przypadku wystąpienia jakiegokolwiek zakłócenia. Organizacje posiadające odporność, nieustannie pracują nad dostosowaniem się do zachodzących zmian i związanego ze zmianami ryzyka, które mogą wpłynąć na ich zdolność do kontynuowania kluczowych funkcji. Zarządzanie ryzykiem (*ang. Risk Management*), planowanie awaryjne i planowanie ciągłości to podstawowe działania w zakresie bezpieczeństwa i zarządzania kryzysowego, które powinny zostać wdrażać w sposób holistyczny w całej organizacji jako elementy programu odporności.

Skuteczne planowanie awaryjne rozpoczyna się od opracowania polityki planowania awaryjnego organizacji i poddania każdego systemu informatycznego analizie wpływu na działalność (BIA). Ułatwia to ustalanie priorytetów dla systemów i procesów i opracowanie, w celu minimalizacji strat, strategii priorytetów odzyskiwania. Niezbędne jest określenie wpływu zakłócenia pracy systemu informatycznego na operacje i aktywa organizacji, osoby fizyczne, inne organizacje i społeczeństwo poprzez formułę, która analizuje trzy atrybuty bezpieczeństwa: poufność, integralność i dostępność.

- Poufność zapewnia autoryzowane ograniczenia dostępu do informacji i ich ujawniania, w tym środki ochrony prywatności i informacji stanowiących tajemnicę.
- Integralność zabezpiecza przed niewłaściwą modyfikacją lub zniszczeniem informacji i obejmuje zapewnienie niezaprzeczalności i autentyczności informacji.
- Dostępność zapewnia terminowy i niezawodny dostęp do informacji w celu ich wykorzystania.

Dla każdego atrybutu bezpieczeństwa wpływ zakłócenia jest określany jako wysoki, umiarkowany lub niski. Najwyższy z poziomów wpływu na poszczególne atrybuty bezpieczeństwa służy do określenia całościowego poziomu wpływu na bezpieczeństwo systemu informatycznego.

Zagadnienia i strategie planowania awaryjnego dotyczą poziomu wpływu na atrybut bezpieczeństwa związany z dostępnością systemów informatycznych. Strategie dla wysokowydajnych systemów informatycznych powinny uwzględniać opcje wysokiej

dostępności i redundancji. Opcje mogą obejmować w pełni redundantne systemy z równoważeniem obciążenia w alternatywnych lokalizacjach, dublowanie danych i replikację bazy danych poza siedzibą. Opcje wysokiej dostępności są zwykle drogie w konfiguracji, obsłudze i konserwacji i należy je brać pod uwagę tylko w przypadku systemów informatycznych o dużym wpływie, sklasyfikowanych w kategoriach atrybutu bezpieczeństwa w zakresie wysokiej dostępności. Systemy informacyjne o mniejszym wpływie mogą korzystać z tańszych opcji awaryjnych i tolerować dłuższe przestoje w celu odzyskiwania lub przywracania danych.

Skuteczne planowanie awaryjne obejmuje wprowadzenie zabezpieczeń na wczesnym etapie rozwoju systemu informatycznego i utrzymywanie tych zabezpieczeń na bieżąco. NSC 800-53, określa dwanaście (zabezpieczenia posiadają numerację od CP-1 do CP-13, z tym że zabezpieczenie CP-5 zostało wycofane w najnowszym wydaniu NSC 800-53) kategorii zabezpieczeń systemów informatycznych w ramach planowania awaryjnego (CP). Nie wszystkie zabezpieczenia mają zastosowanie do wszystkich systemów. Kategoryzacja wpływu zakłócenia określa, które zabezpieczenia mają zastosowanie do konkretnego systemu. Na przykład systemy informatyczne, które mają dostępność jako atrybut bezpieczeństwa sklasyfikowany jako mało istotny, nie wymagają alternatywnych miejsc przetwarzania lub przechowywania, a systemy informatyczne, które mają ten atrybut bezpieczeństwa zaklasyfikowany jako podlegający wpływowi umiarkowanemu, wymagają zgodności tylko z pierwszymi rozszerzeniami zabezpieczeń w zakresie tworzenia kopii zapasowych systemu. Zastosowanie kategoryzacji wpływu zakłócenia na bezpieczeństwo pozwala na zastosowanie zabezpieczeń planowania awaryjnego (*ang. Contingency planning – CP*) zawartych w NSC 800-53 do tych, które spełniają podstawowe wymagania. Tabela 2-1 zawiera podsumowanie zabezpieczeń planowania awaryjnego z NSC 800-53 i ich zastosowanie do podstawowych zabezpieczeń. Dalsze szczegóły i opisy zabezpieczeń planowania awaryjnego znajdują się w załączniku E.

Kilka zabezpieczeń CP odnosi się do zabezpieczeń środowiska, które są częścią kategorii zabezpieczeń NSC 800-53 *Ochrona fizyczna i środowiskowa (ang. Physical and environmental protection - PE)*. Uwagi dotyczące zabezpieczeń środowiska dotyczą tylko lokalizacji lub

budynku, w którym mieści się system informatyczny. Środowisko obejmuje zasoby sprzętowe i technologiczne obsługujące system informatyczny.

Dla organizacji dostępne są opcje ułatwiające stosowanie zabezpieczeń rodziny CP. NSC 800-53 pozwala na zastosowanie zamiennych zabezpieczeń w celu zapewnienia ochrony dla systemu informatycznego zgodnego z intencją zabezpieczeń CP. Organizacja może zastosować zamienne zabezpieczenia zamiast zabezpieczeń CP, o ile istnieje uzasadnienie dla zastosowania zabezpieczenia zamiennego i chęć zaakceptowania ryzyka wdrożenia zabezpieczenia zamiennego.

**Tabela 2-1: Podsumowanie zabezpieczeń planowania awaryjnego NSC 800-53 w przypadku systemów planów awaryjnych o niskim, umiarkowanym i wysokim wpływie zakłócenia na bezpieczeństwo[4]**

| Identyfikator zabezpieczenia | Nazwa zabezpieczenia | Zabezpieczenie i jego rozszerzenia | | |
|---|---|---|---|---|
| | | Niski | Umiarkowany | Wysoki |
| CP-1 | Polityka i procedury | CP-1 | CP-1 | CP-1 |
| CP-2 | Plan ciągłości działania | CP-2 | CP-2 (1) | CP-2 (1) (2) (3) |
| CP-3 | Szkolenia w zakresie planowania ciągłości działania | CP-3 | CP-3 | CP-3 (1) |
| CP-4 | Testowanie planu ciągłości działania | CP-4 | CP-4 (1) | CP-4 (1) (2) (4) |
| CP-5 | Aktualizacja planu awaryjnego (wycofane) | ------ | ----- | ------ |

[4] Liczby w nawiasach wskazują na numer zabezpieczenia rozszerzonego

| Identyfikator zabezpieczenia | Nazwa zabezpieczenia | Zabezpieczenie i jego rozszerzenia | | |
|---|---|---|---|---|
| | | Niski | Umiarkowany | Wysoki |
| CP-6 | Zapasowe miejsce przechowywania kopii | Nie jest wymagane | CP-6 (1) (3) | CP-6 (1) (2) (3) |
| CP-7 | Zapasowe miejsce przetwarzania | Nie jest wymagane | CP-7 (1) (2) (3) (5) | CP-7 (1) (2) (3) (4) (5) |
| CP-8 | Usługi telekomunikacyjne | Nie jest wymagane | CP-8 (1) (2) | CP-8 (1) (2) (3) (4) |
| CP-9 | Kopia zapasowa | CP-9 | CP-9 (1) | CP-9 (1) (2) (3) |
| CP-10 | Odzyskiwanie i odtwarzanie systemu | CP-10 | CP-10 (2) (3) | CP-10 (2) (3) (4) |
| CP-11 | Alternatywne protokoły komunikacji | CP-11 | CP-11 | CP-11 |
| CP-12 | Tryb bezpieczny | Nie jest wymagane | CP-12 | CP-12 |
| CP-13 | Alternatywne mechanizmy bezpieczeństwa | Nie jest wymagane | Nie jest wymagane | CP-13 |

## 2.2 RODZAJE PLANÓW

Planowanie awaryjne systemu informatycznego obejmuje szeroki zakres działań mających na celu utrzymanie i odzyskanie krytycznych usług systemowych po zdarzeniu awaryjnym. Planowanie awaryjne w systemie informatycznym stanowi znacznie szerszy zakres działań związanych z zarządzaniem bezpieczeństwem i sytuacjami kryzysowymi, które dotyczą ciągłości procesów organizacyjnych i biznesowych, niż planowanie odzyskiwania po awarii oraz zarządzanie incydentami. Konkludując, organizacja użyłaby zestawu planów, aby odpowiednio przeprowadzić działania reagowania, odzyskiwania i ciągłości na wypadek

zakłóceń wpływających na systemy informacyjne organizacji, procesy związane z celem działania, personelem i siedzibą. Ponieważ istnieje nieodłączny związek między systemem informatycznym, a wspieranymi przez niego procesami z zakresu działalności organizacji, podczas opracowywania i aktualizacji planów musi istnieć koordynacja między wszystkimi planami, aby zapewnić, że strategie odzyskiwania i zasoby pomocnicze nie będą się wzajemnie negować lub nie będą powielać działań.

Ciągłość działania i planowanie awaryjne są kluczowymi elementami zarządzania kryzysowego i odporności organizacyjnej, ale ich stosowanie jest często mylone. Planowanie ciągłości działania zwykle dotyczy samego celu działalności organizacji i obejmuje zdolności do kontynuowania krytycznych funkcji i procesów w trakcie i po zdarzeniu awaryjnym. Planowanie awaryjne dotyczy zaś systemów informatycznych i zapewnia kroki niezbędne do przywrócenia działania wszystkich lub części wyznaczonych systemów informatycznych w istniejącym lub nowym miejscu w sytuacji awaryjnej. Planowanie reagowania na incydenty cyberbezpieczeństwa to rodzaj planu, który zwykle koncentruje się na wykrywaniu, reagowaniu i odzyskiwaniu danych po incydencie lub zdarzeniu związanym z bezpieczeństwem informacji.

Zasadniczo, uniwersalne, powszechnie akceptowane definicje planowania awaryjnego systemu informacyjnego i powiązanych z tym obszarów planowania, nie są dostępne. Czasami prowadzi to do nieporozumień co do faktycznego zakresu i celu różnych rodzajów planów. Aby zapewnić wspólną podstawę do zrozumienia planowania awaryjnego systemu informatycznego, w tej sekcji wymieniono kilka innych rodzajów planów oraz opisano ich cel i zakres w odniesieniu do planowania awaryjnego systemu informatycznego. Z powodu braku standardowych definicji dla tego rodzaju planów, zakres rzeczywistych planów opracowanych przez organizacje może różnić się od poniższych opisów. Niniejszy przewodnik w kolejnych sekcjach stosuje opisy i odniesienia do planów związanych z bezpieczeństwem i zarządzaniem kryzysowym. Kolejność wymienienia planów nie sugeruje ich ważności.

### 2.2.1 PLAN CIĄGŁOŚCI DZIAŁANIA (*BUSINESS CONTINUITY PLAN – BCP*)

BCP koncentruje się na utrzymaniu procesów biznesowych organizacji w trakcie i po zakłóceniu. Przykładem procesu biznesowego może być proces płacowy organizacji lub proces obsługi klienta. BCP może być napisany dla procesów biznesowych w ramach jednej komórki organizacyjnej lub może dotyczyć procesów całej organizacji. Zakres BCP może obejmować jedynie funkcje uznane za priorytetowe. BCP można wykorzystać do długoterminowego odzyskiwania w połączeniu z planem COOP, pozwalając na włączenie dodatkowych funkcji w miarę zasobów lub dozwolonego czasu. Ponieważ procesy biznesowe wykorzystują systemy informatyczne (SI), planista ciągłości działania musi koordynować swój plan z właścicielami systemów informatycznych, tak aby zapewnić zgodność oczekiwań BCP i możliwości SI.

### 2.2.2 PLAN KONTYNUACJI OPERACJI (*CONTINUITY OF OPERATIONS PLAN – COOP*)

COOP koncentruje się na przywróceniu kluczowych funkcji organizacji (*ang. Mission Essential Functions – MEF*) w alternatywnej lokalizacji i wykonywaniu tych funkcji przez 30 dni przed powrotem do normalnej działalności. Dodatkowe funkcje lub funkcje na poziomie lokalizacji terenowej mogą być realizowane przez BCP. Drobne zagrożenia lub zakłócenia, które nie wymagają przeniesienia do innej lokalizacji, zazwyczaj nie są uwzględniane w planie COOP.

Standardowe elementy planu COOP obejmują:

- Program planu i procedury;
- Zarządzanie ryzykiem;
- Budżetowanie i pozyskiwanie zasobów;
- Kluczowe funkcje objęte planem;
- Ustanowienie zastępstw;
- Przekazanie uprawnień;
- Obiekty (lokalizacje) zapewniające ciągłość;
- Ciągłość komunikacji;

- Zarządzanie niezbędnymi zapisami;
- Zasoby ludzkie;
- Test, trening i ćwiczenia;
- Zasady przeniesienia przetwarzania do miejsca zapasowego;
- Zasady powrotu do pracy w lokalizacji podstawowej.

### 2.2.3 PLAN KOMUNIKACJI KRYZYSOWEJ (*CRISIS COMMUNICATIONS PLAN*)

Organizacje powinny udokumentować standardowe procedury komunikacji wewnętrznej i zewnętrznej w przypadku wystąpienia zakłócenia, poprzez ustanowienie planu komunikacji kryzysowej. W szczególności plan komunikacji kryzysowej powinien być opracowany przez organizacje prowadzące działalność publiczną. Plan powinien zawierać różne formy komunikacji, odpowiednie do danego zdarzenia. Plan komunikacji kryzysowej zazwyczaj wyznacza określone osoby jako jedyne, odpowiedzialne za udzielanie odpowiedzi na pytania zewnętrzne, a w szczególności informowania społeczeństwa na temat reakcji w sytuacjach kryzysowych. Może to również obejmować procedury przekazywania pracownikom raportów o stanie incydentu oraz szablony publicznych komunikatów prasowych. Procedury planu komunikacji kryzysowej powinny być przekazywane organizatorom COOP i BCP tak, aby zapewnić, że plany te zawierają wyraźne wytyczne co do spójnego sposobu komunikowania się z otoczeniem. Dodatek D zawiera dalsze omówienie tematów poruszonych w planie komunikacji kryzysowej.

### 2.2.4 PLAN OCHRONY INFRASTRUKTURY KRYTYCZNEJ (*CRITICAL INFRASTRUCTURE PROTECTION PLAN – CIP*)

Krytyczna infrastruktura i kluczowe zasoby (*ang. Critical infrastructure and key resources - CIKR*) to te elementy infrastruktury krajowej, które uważa się za tak istotne, ponieważ ich utrata miałaby wyniszczający wpływ na bezpieczeństwo, ochronę, ekonomię lub zdrowie w Państwie. Plan CIP jest zestawem zasad i procedur służących ochronie i odzyskiwaniu tych zasobów krajowych oraz usuwaniu podatności i ograniczaniu ryzyka. Plany CIP określają role i obowiązki w zakresie ochrony, rozwijają partnerstwa i relacje w zakresie wymiany

informacji, wdrażają ramy zarządzania ryzykiem określone w Krajowym planie ochrony infrastruktury Krytycznej NPOIK (*ang. National Infrastructure Protection Plan - NIPP*). Tworzenie CIP jest uregulowane przepisami ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym i przepisami wykonawczymi do tej ustawy.

### 2.2.5 PLAN ODPOWIEDZI NA INCYDENTY CYBERBEZPIECZEŃSTWA (*CYBER INCIDENT RESPONSE PLAN - CIRP*)

Plan reagowania na incydenty cyberbezpieczeństwa ustanawia procedury przeciwdziałania atakom pochodzącym z cyberprzestrzeni na systemy informatyczne organizacji. Procedury te powinny zostać tak zaprojektowane, aby umożliwić personelowi zajmującemu się ochroną systemów zidentyfikowanie, złagodzenie skutków w czasie i po atakach, takich jak nieautoryzowany dostęp do systemu lub danych, odmowa usługi lub nieautoryzowane zmiany w sprzęcie, oprogramowaniu lub danych systemowych (np. złośliwa logika, taka jak wirus, robak lub koń trojański), a także ustalenie zasięgu ataku, zabezpieczenie śladów kryminalistycznych i odzyskanie danych, jeśli doszło do ich utraty, albo możliwości dostępu do nich. Plan ten może być zawarty, jako załącznik do BCP.

### 2.2.6 PLAN ODTWORZENIA PO KATASTROFIE (*DISASTER RECOVERY PLAN – DRP*)

DRP ma zastosowanie do poważnych, zwykle fizycznych zakłóceń świadczenia usługi, które uniemożliwiają dostęp do podstawowej infrastruktury obiektu przez dłuższy okres. DRP jest planem skoncentrowanym na systemie informatycznym, mającym na celu przywrócenie działania docelowej infrastruktury systemu, aplikacji lub infrastruktury komputerowej w alternatywnym miejscu po awarii. DRP może być wspierany przez plany awaryjne poszczególnych systemów informatycznych, dotyczące odzyskiwania pojedynczych systemów, na które ma wpływ przejście do pracy w obiekcie alternatywnym. DRP może wspierać plan BCP lub COOP, odzyskując systemy wspierające działanie procesów biznesowych lub podstawowych funkcji celu działania organizacji w alternatywnej lokalizacji. DRP usuwa tylko zakłócenia pracy przenoszonego systemu informatycznego.

### 2.2.7 PLAN AWARYJNY SYSTEMU INFORMATYCZNEGO (*INFORMATION SYSTEM CONTINGENCY PLAN – ISCP*)

ISCP zapewnia ustanowienie procedur oceny i odzyskiwania systemu po jego awarii. ISCP zapewnia kluczowe informacje potrzebne do odzyskiwania systemu, w tym role i obowiązki, informacje o zasobach, procedury oceny sytuacji, szczegółowe procedury odzyskiwania i testowanie systemu.

ISCP różni się od DRP przede wszystkim tym, że procedury planu awaryjnego systemu informatycznego mają na celu odzyskanie systemu niezależnie od lokalizacji. ISCP można aktywować w bieżącej lokalizacji systemu lub w dowolnej innej. Natomiast DRP to przede wszystkim plan specyficzny dla danego miejsca, opracowany z procedurami przenoszenia operacji jednego lub więcej systemów informatycznych z uszkodzonej lub niezdatnej do wykorzystywania lokalizacji do tymczasowej lokalizacji alternatywnej. Po tym, jak DRP pomyślnie przeniesie zasoby systemu informatycznego do innej lokalizacji, każdy z systemów, którego dotyczy problem, użyje odpowiedniego ISCP w celu przywrócenia sprawności i przetestowanie systemów oraz ich produkcyjne udostępnienie.

### 2.2.8 PLAN EWAKUACJI (*OCCUPANT EMERGENCY PLAN – OEP*)

OEP określa procedury pierwszej reakcji przeznaczone dla osób przebywających w obiekcie na wypadek zagrożenia lub incydentu dla zdrowia i bezpieczeństwa personelu, środowiska lub mienia. Takie zdarzenia obejmują pożar, zagrożenie bombowe, uwolnienie substancji chemicznych, przemoc fizyczną w miejscu pracy lub nagły wypadek medyczny. Procedury te mogą również obejmować chronienie się personelu w bezpiecznych pomieszczeniach, zamiast ewakuacji. OEP są opracowywane na poziomie obiektu, specyficzne dla położenia geograficznego i projektu konstrukcyjnego budynku. OEP organizacji może być dołączony do COOP lub BCP, ale jest wykonywany osobno i jako pierwsza odpowiedź na zdarzenie. Aspekty planowania bezpieczeństwa personelu i ewakuacji omówiono w załączniku D.

**Tabela 2-2: Typy Planów**

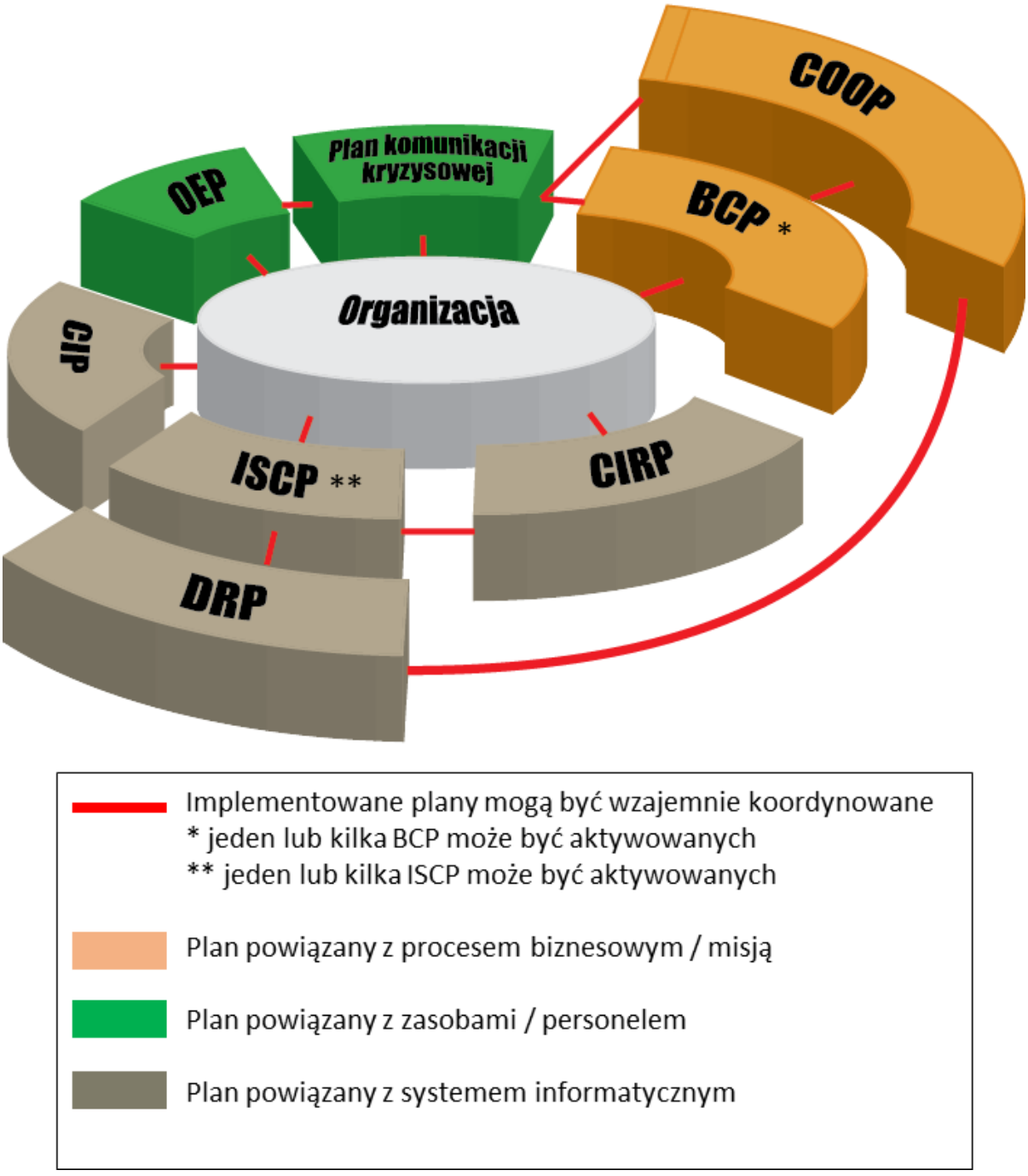
| Plan | Cel | Zakres | Relacja pomiędzy planami |
|---|---|---|---|
| Plan ciągłości działania (*Business Continuity Plan – BCP*) | Zapewnia procedury podtrzymywania operacji biznesowych podczas ich odzyskiwania po znacznych zakłóceniach. | Adresowany do procesów biznesowych na niższym lub rozszerzonym poziomie w stosunku do COOP MEF. | Plan zorientowany na procesy biznesowe, który może zostać aktywowany łącznie z planem COOP w celu utrzymania funkcjonalności innych niż MEF. |
| Plan ciągłości operacji (*Continuity of Operations Plan – COOP*) | Zapewnia procedury i wytyczne w celu utrzymania MEF organizacji w alternatywnej lokalizacji przez okres do 30 dni. | Adresowany do MEF w obiekcie; systemy informatyczne są przeznaczone wyłącznie do wsparcia podstawowych funkcji celu działania organizacji. | Plan skoncentrowany na MEF, może również aktywować BCP dla określonych procesów biznesowych, ISCP lub DRP, zależnie od przypadku. |

| Plan | Cel | Zakres | Relacja pomiędzy planami |
|---|---|---|---|
| Plan komunikacji kryzysowej (*Crisis Communications Plan*) | Zapewnia procedury rozpowszechniania komunikacji wewnętrznej i zewnętrznej w celu dostarczania krytycznych informacji o stanie organizacji i przeciwdziałaniu pogłoskom. | Adresuje komunikację z personelem i społeczeństwem; nie koncentruje się na systemie informatycznym. | Plan aktywowany przez incydent, często za pomocą COOP lub BCP, ale może być stosowany samodzielnie podczas zdarzenia naruszającego wizerunek organizacji. |
| Plan ochrony infrastruktury krytycznej (*Critical Infrastructure Protection Plan – CIP*) | Zapewnia zasady i procedury ochrony krajowych elementów infrastruktury krytycznej, zgodnie z definicją w krajowym planie ochrony infrastruktury. | Adresowany do krytycznych elementów infrastruktury państwa. | Plan zarządzania ryzykiem występujący w planach COOP w organizacjach posiadających infrastrukturę krytyczną i zasoby kluczowe. |

| Plan | Cel | Zakres | Relacja pomiędzy planami |
|---|---|---|---|
| Plan odpowiedzi na incydenty cyberbezpieczeństwa *(Cyber Incident Response Plan - CIRP)* | Zapewnia procedury ograniczania i korygowania cyberataku, takiego jak wirus, robak lub koń trojański. | Rozwiązuje problem ograniczania incydentu i izolacji systemów, których dotyczy incydent, usuwania oprogramowania szkodliwego i minimalizacji utraty informacji. | Plan zorientowany na system informatyczny, może aktywować ISCP lub DRP, w zależności od zasięgu ataku. |
| Plan odtworzenia po katastrofie (*Disaster Recovery Plan – DRP*) | Zapewnia procedury przenoszenia operacji systemów informatycznych do innej lokalizacji. | Aktywowany po poważnych zakłóceniach systemu z długoterminowymi skutkami. | Plan zorientowany na system informatyczny, który aktywuje jeden lub więcej ISCP w celu odzyskiwania poszczególnych systemów. |

| Plan | Cel | Zakres | Relacja pomiędzy planami |
|---|---|---|---|
| Plan awaryjny systemu informatycznego (*Information System Contingency Plan – ISCP*) | Zapewnia procedury i możliwości odzyskiwania systemu informatycznego. | Rozwiązuje problem odzyskiwania pojedynczego systemu informatycznego w bieżącej lub, w razie potrzeby, w innej lokalizacji. | Plan zorientowany na system informatyczny, który może być aktywowany niezależnie od innych planów lub w ramach większego wysiłku naprawczego skoordynowanego z DRP, COOP i / lub BCP. |
| Plan ewakuacji (*Occupant Emergency Plan – OEP*) | Zapewnia skoordynowane procedury w celu zminimalizowania utraty życia lub obrażeń oraz zapobiega szkodom materialnym w odpowiedzi na zagrożenie fizyczne. | Koncentruje się na personelu i infrastrukturze budynku, specyficznych dla konkretnego obiektu; nie jest związany z procesem biznesowym lub systemem informatycznym. | Plan związany z incydentem, który jest inicjowany natychmiast po zdarzeniu, poprzedza aktywację COOP lub DRP. |

Rysunek 2-1 ilustruje wzajemne powiązania poszczególnych planów podczas wdrażania w odpowiedzi na zdarzenie, stosownie do ich zakresów.



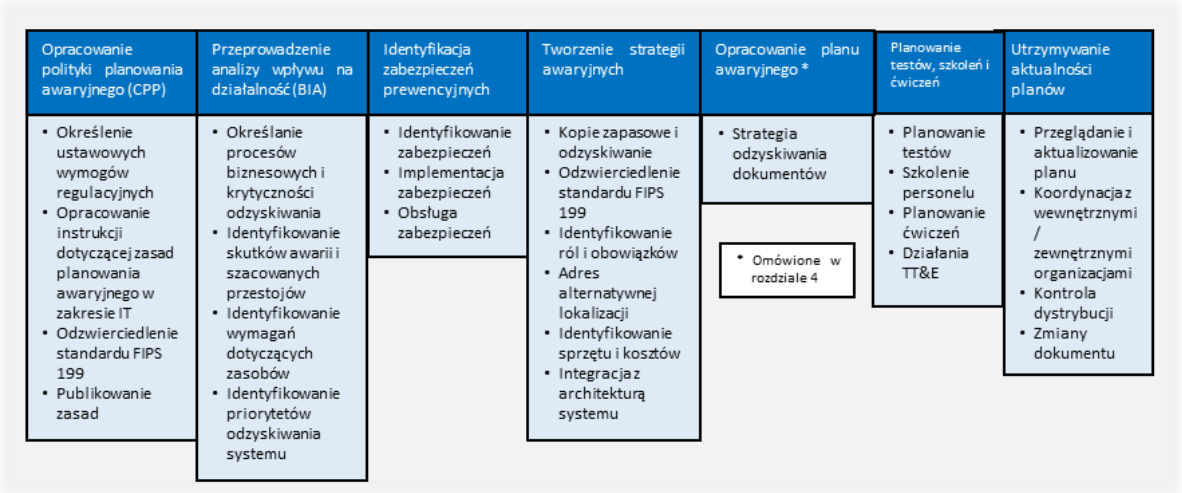

**Rysunek 2-1 Relacje pomiędzy planami**

# ROZDZIAŁ 3 PROCES PLANOWANIA AWARYJNEGO DLA SYSTEMU INFORMATYCZNEGO

W tej części opisano proces opracowywania i utrzymywania skutecznego planu awaryjnego systemu informacyjnego. Przedstawiony proces jest wspólny dla wszystkich systemów informatycznych. Siedem kroków tego procesu to:

1. Opracowanie polityki planowania awaryjnego;
2. Przeprowadzenie analizy wpływu na działalność (BIA);
3. Identyfikacja zabezpieczeń prewencyjnych;
4. Utworzenie strategii awaryjnych;
5. Opracowanie planu awaryjnego systemu informatycznego;
6. Zaplanowanie testów, szkoleń i ćwiczeń;
7. Zapewnienie utrzymywania planów w aktualności.

Kroki te stanowią kluczowe elementy kompleksowego systemu planowania awaryjnego systemu informatycznego. Opracowanie polityki planowania awaryjnego i wykonanie BIA systemu wykonuje się na wczesnym etapie w SDLC (patrz Załącznik F), a przed klasyfikacją systemów zgodnie z RMF. W tym rozdziale omówiono sześć z siedmiu etapów procesu planowania. Ponieważ opracowanie planu stanowi rdzeń planowania awaryjnego systemu informatycznego, w tym poszczególnych sekcji, które składają się na plan, opracowanie planu opisano w rozdziale 4. Odpowiedzialność za proces planowania zasadniczo spoczywa na koordynatorze planu awaryjnego systemu informatycznego lub koordynatorze ISCP , który zazwyczaj jest funkcjonalnym lub zarządzającym zasobami w organizacji. Koordynator ISCP opracowuje strategię we współpracy z innymi menedżerami funkcjonalnymi i zarządzającymi zasobami związanymi z systemem lub obsługiwanymi przez system procesami biznesowymi. Koordynator ISCP zazwyczaj również zarządza opracowaniem i realizacją planu awaryjnego. Wszystkie systemy informatyczne podmiotów publicznych muszą mieć plan awaryjny. Rysunek 3-1 ilustruje proces planowania awaryjnego.




**Rysunek 3-1 Proces planowania awaryjnego**

## 3.1 DEKLARACJA ZASAD PLANOWANIA AWARYJNEGO

Aby być skutecznym i zapewnić, że personel w pełni rozumie wymagania organizacji w zakresie planowania awaryjnego plan awaryjny musi opierać się na jasno określonych zasadach. Deklaracja polityki planowania awaryjnego powinna określać ogólne cele organizacji na wypadek awarii oraz określać ramy organizacyjne i obowiązki związane z planowaniem awaryjnym systemu. Aby odnieść sukces, kierownictwo wyższego szczebla musi wspierać program awaryjny i brać udział w procesie opracowywania polityki programu awaryjnego. Polityka musi odzwierciedlać poziomy wpływu incydentu na bezpieczeństwo informacji oraz zabezpieczenia na wypadek awarii ustanowione dla każdego poziomu wpływu. Kluczowe elementy polityki są następujące:

- Role i obowiązki;
- Zakres, jaki ma zastosowanie do wspólnych rodzajów platform i funkcji organizacyjnych (tj. telekomunikacja, kwestie prawne, relacje z mediami), będących przedmiotem planowania awaryjnego;
- Wymagania dotyczące zasobów;
- Wymagania szkoleniowe;

- Harmonogramy ćwiczeń i testów;
- Harmonogram utrzymania planów;
- Minimalna częstotliwość tworzenia kopii zapasowych i sposoby przechowywania nośników kopii zapasowych.

**Przykładowe oświadczenie dotyczące polityki awaryjnej systemu informacyjnego**

Wszystkie organizacje muszą opracować plany awaryjne dla każdego systemu informatycznego, tak, aby zaspokoić potrzeby krytycznych operacji w przypadku zakłócenia pracy systemu. Procedury realizacji takiej zdolności muszą być udokumentowane przez koordynatora planu awaryjnego systemów informatycznych (ISCP) w planie awaryjnym i muszą być corocznie przeglądane i aktualizowane w razie potrzeby przez koordynatora ISCP. Plan musi uwzględniać kategoryzację bezpieczeństwa z uwzględnieniem poziomu wpływu zakłócenia na bezpieczeństwo informacji (niski, umiarkowany, wysoki) i uwzględniać zastosowane zabezpieczenia. W celu ułatwienia przywracania lub zapewnienia ciągłości podstawowych funkcji systemu, plan musi przypisywać określone obowiązki wyznaczonemu personelowi lub stanowiskom w organizacji. Muszą zostać pozyskane i utrzymane zasoby niezbędne do zapewnienia wykonalności procedur. Personel odpowiedzialny za systemy docelowe musi zostać przeszkolony w zakresie wykonywania procedur awaryjnych. Zdolności do wykonania planu przez personel są corocznie testowane w celu wykrycia jego słabych punktów.

Ponieważ plany awaryjne systemu informatycznego są opracowywane podczas fazy inicjowania SDLC[5], należy je skoordynować w powiązaniu z zasadami obejmującymi całą organizację, w tym dotyczącymi bezpieczeństwa systemu informatycznego, bezpieczeństwa fizycznego, zasobów ludzkich, operacji w systemie i funkcjami gotowości na wypadek awarii.

[5] SDLC odnosi się do zakresu działań związanych z systemem, obejmujących inicjowanie, rozwój i nabywanie, wdrażanie, eksploatacją i konserwację systemu, a ostatecznie jego zbycie, które stanowi podstawę do inicjacji innego systemu. Podejście SDLC jest szczegółowo omówione w standardzie "Zagadnienia dotyczące zabezpieczeń w cyklu życia systemu informacyjnego - NSC 800-64". Przegląd planowania awaryjnego i SDLC przedstawiono w Załączniku F.

Działania awaryjne systemu informatycznego powinny być zgodne z wymogami zasad dla tych obszarów, a personel ds. odzyskiwania powinien koordynować działania z przedstawicielami każdego obszaru, aby mieć świadomość nowych lub ewoluujących zasad lub możliwości. ISCP muszą być napisane w koordynacji z innymi planami związanymi z każdym systemem docelowym w ramach strategii odporności dla całej organizacji. Takie plany obejmują:

- Plany bezpieczeństwa systemów informatycznych;
- Plany na poziomie obiektu, takie jak OEP i DRP;
- Wsparcie MEF, takie jak plan COOP;
- Plany na poziomie organizacji, takie jak plany CIP.

Podobnie, sześciostopniowe RMF scalają wykorzystywane standardy bezpieczeństwa oraz wytyczne niezbędne do zarządzania ryzykiem związanym z systemami informatycznymi. Wdrożenie RMF w systemie informatycznym obejmuje szeroki zakres działań w celu szacowania i ograniczania ryzyka. Z perspektywy planowania awaryjnego systemu informatycznego sześć kroków w RMF aktywnie wspiera rozwój, wdrażanie, testowanie i utrzymanie planu awaryjnego systemu informatycznego, ponieważ wspiera on misję organizacji.

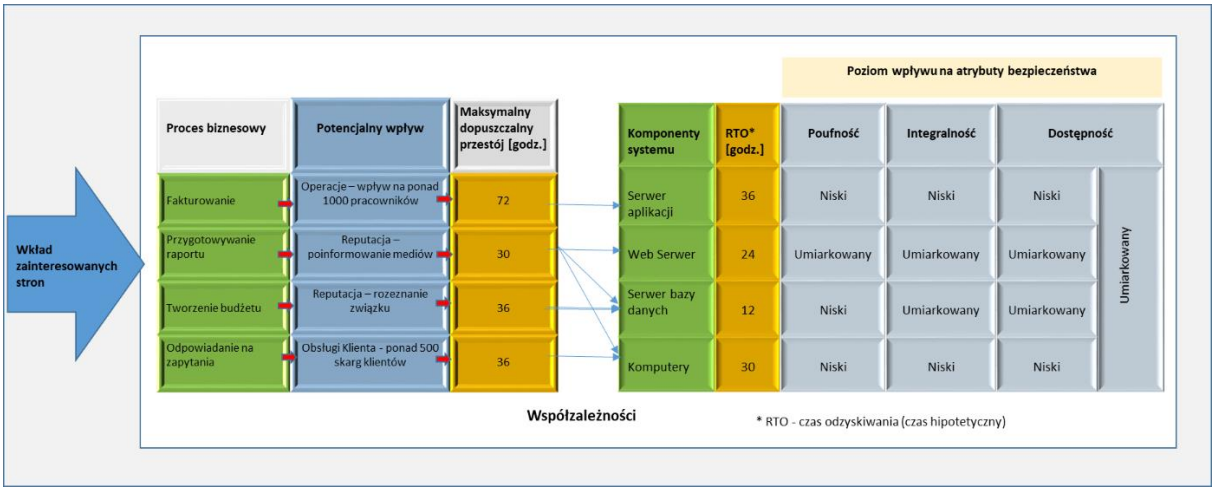
BIA jest kluczowym krokiem we wdrażaniu zabezpieczeń CP zawartych w NSC 800-53 i w całym procesie planowania awaryjnego. BIA umożliwia koordynatorowi ISCP scharakteryzowanie komponentów systemu, obsługiwanych procesów biznesowych oraz występujących współzależności. Celem BIA jest skorelowanie systemu z kluczowymi procesami oraz świadczonymi usługami biznesowymi, a na podstawie tych informacji scharakteryzowanie konsekwencji wynikających z zakłócenia pracy systemu. Koordynator ISCP może wykorzystać wyniki BIA do ustalenia wymagań i priorytetów planowania awaryjnego. Wyniki BIA powinny być odpowiednio uwzględnione w analizie i opracowywaniu strategii dla COOP organizacji, BCP i DRP. BIA należy wykonać podczas fazy inicjacji SDLC. W miarę ewolucji systemu i zmian komponentów, BIA może wymagać ponownego przeprowadzenia podczas fazy rozwoju SDLC. Włączenie RMF w Etapie 1

(kategoryzacja poziomu wpływu zakłócenia na bezpieczeństwo informacji) i Etapie 2 (wybrane zabezpieczenia) pomaga zapewnić, że BIA odpowiednio uwzględnia poziomy ryzyka występujące organizacji.

Przeprowadzenie BIA zazwyczaj wymaga następujących trzech kroków:

1. **Określanie procesów biznesowych i krytyczności ich odzyskiwania.** Identyfikowane są procesy biznesowe wspierane przez system, a wpływ awarii systemu na te procesy jest określany wraz ze skutkami awarii i szacowanym czasem przestoju. Przestoje powinny odzwierciedlać maksymalny czas, który organizacja może tolerować przy jednoczesnym utrzymaniu celu swojego działania.
2. **Identyfikacja wymagań dotyczących zasobów.** Realistyczne działania naprawcze wymagają dokładnej oceny zasobów wymaganych do wznowienia głównych procesów biznesowych i powiązanych z nimi współzależności, tak szybko jak to jest możliwe. Przykładowe zasoby, które należy zidentyfikować, to: obiekty, personel, sprzęt, oprogramowanie, pliki danych, komponenty systemu i niezbędne zapisy.
3. **Określenie priorytetów odzyskiwania zasobów systemowych.** W oparciu o wyniki poprzednich działań, zasoby systemowe można wyraźniej powiązać z krytycznymi procesami i funkcjami biznesowymi i w ten sposób ustalić poziomy priorytetów dla ustalenia kolejności działań mających na celu odzyskiwanie zasobów.

Przykładowy proces BIA, w tym działania związane z gromadzeniem danych, przedstawione w tym rozdziale i zilustrowane na rysunku 3-2, odnoszą się do reprezentatywnego systemu informatycznego z wieloma komponentami (serwerami) i mają na celu pomóc koordynatorowi ISCP w usprawnieniu działań związanych z opracowaniem planu awaryjnego. Przykład procesu BIA i szablon BIA znajdują się w załączniku B.




**Rysunek 3- 2 Proces analizy wpływu na biznes dla systemu informacyjnego**

### 3.2.1 OKREŚLANIE PROCESÓW BIZNESOWYCH I KRYTYCZNOŚĆ ODZYSKIWANIA

System informatyczny może być bardzo złożony i często obsługuje wiele procesów biznesowych, co daje różny punkt widzenia na znaczenie usług systemowych. Aby przeprowadzić BIA i lepiej zrozumieć wpływ awarii lub zakłóceń pracy systemu na organizację, koordynator ISCP w celu zidentyfikowania i uzgodnienia procesów biznesowych, które są zależne od systemu informatycznego lub przez niego wspierane, powinien współpracować z zarządem oraz wewnętrznymi i zewnętrznymi punktami kontaktowymi (PoC). Wpływ zakłócenia pracy systemu informatycznego na zidentyfikowane procesy jest następnie analizowany pod względem dostępności, integralności, poufności informacji zgodnie z NSC 199.

NSC 199 wymaga, aby organizacje klasyfikowały swoje systemy informacyjne jako systemy o małym, umiarkowanym lub o wysokim wpływie na atrybuty bezpieczeństwa, takie jak poufność, integralność i dostępność (RMF Krok 1). Kategoria wpływu zakłócenia wg. NSC 199 dla atrybutu bezpieczeństwa jakim jest dostępność, stanowi podstawę BIA. Dalsza identyfikacja procesów dodatkowych i ich wpływów na biznes wynika już z unikatowej charakterystyki danego systemu. Unikatowość organizacyjna i systemowa są ważnymi czynnikami przy planowaniu awaryjnym i wpływie na biznes. Uwzględnienie tego typu

informacji pozwoli na lepsze zrozumienie potrzeb organizacji w zakresie określania priorytetów wpływów zakłócenia na komponenty systemu.

Poszczególne procesy i oddziaływania można wyrazić w wartościach lub jednostkach miary, które są istotne dla organizacji. Wartości można zidentyfikować za pomocą skali i należy je scharakteryzować jako wskaźnik istotności wpływu na organizację w sytuacji, gdy jakiś proces nie może zostać przeprowadzony. Na przykład można utworzyć kategorię wpływu, taką jak „Koszty" z wartościami wpływu wyrażonymi w kategoriach kosztów personelu, nadgodzin lub innych opłat.

Koordynator ISCP powinien następnie przeanalizować obsługiwane procesy biznesowe, a właściciele procesów, kierownictwo i menedżerowie biznesowi określają dopuszczalny czas przestoju, jeśli dany proces lub określone dane systemowe zostały zakłócone lub w inny sposób niedostępne. Przestoje można zidentyfikować na kilka sposobów:

- **Maksymalna tolerowana przerwa** (*ang. Maximum Tolerable Downtime - MTD*).

  MTD reprezentuje całkowity czas, jaki właściciel systemu jest skłonny zaakceptować w związku z przerwaniem lub zakłóceniem procesu biznesowego, uwzględniając wszystkie czynniki dotyczące wpływu przerwy lub zakłócenia na te procesy. Określenie MTD jest ważne, ponieważ jego złe zdefiniowanie może wskazać planistom awaryjnym zły kierunek co do (1) wyboru odpowiedniej metody odzyskiwania oraz (2) istotności szczegółów, które będą brane pod uwagę przy opracowywaniu procedur odzyskiwania, w tym ich zakresu i treści.

- **Czas odzyskania** (*ang. Recovery Time Objective - RTO*).

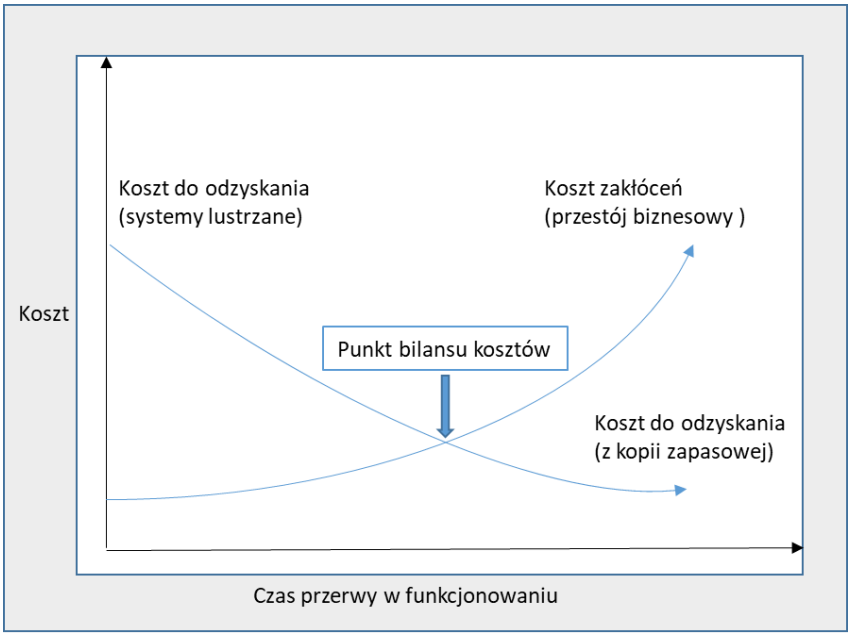
  RTO określa maksymalny czas, przez który zasób systemowy może pozostać niedostępny i będzie miał nieakceptowalny wpływ na inne zasoby systemowe, obsługiwane procesy biznesowe i MTD. Określenie RTO dla danego zasobu systemu informatycznego jest ważne przy wyborze odpowiednich technologii, które najlepiej nadają się do spełnienia MTD. Gdy nie jest możliwe natychmiastowe spełnienie wymagań RTO, a MTD jest nieelastyczne, należy zainicjować plan działania w celu

udokumentowania sytuacji i podjęcie przez kierownictwo decyzji w celu rozwiązania problemu.

- **Punkt odtworzenia danych** (*ang. Recovery Point Objective - RPO*). RPO reprezentuje moment, przed wystąpieniem zakłócenia lub awarii systemu, od którego można odzyskać dane procesu biznesowego (biorąc pod uwagę najnowszą kopię zapasową danych) po zaistnieniu awarii. W przeciwieństwie do RTO, RPO nie jest uważane za część MTD. Jest to raczej czynnik określający, jaką utratę danych toleruje proces biznesowy podczas procesu odzyskiwania.

Ponieważ RTO musi zapewnić, że MTD nie zostanie przekroczony, RTO zwykle musi być krótszy niż MTD. Na przykład awaria systemu może uniemożliwić zakończenie określonego procesu, a ponieważ ponowne przetworzenie danych wymaga czasu, aby utrzymać się w limicie czasu ustalonym przez MTD, do RTO musi zostać dodany dodatkowy czas potrzebny na to przetwarzanie.

Koordynator ISCP, współpracując z kierownictwem organizacji, powinien określić optymalny punkt do odzyskania systemu informatycznego, uwzględniając powyższe czynniki, równoważąc jednocześnie koszt niedziałania systemu z kosztem zasobów wymaganych do przywrócenia systemu i jego ogólnego wsparcia dla krytycznych procesów biznesowych. Można to zilustrować za pomocą prostej zależności pokazanej na rysunku 3-3.




**Rysunek 3- 3 Równowaga kosztów**

Im dłużej będą trwać zakłócenia, tym bardziej kosztowne może być to dla organizacji i jej działalności. I odwrotnie, im krótszy jest RTO, tym droższe są koszty wdrożenia rozwiązań odzyskiwania. Na przykład, jeśli system musi zostać natychmiast przywrócony (zero przestojów), to koszty alternatywnego miejsca przetwarzania będą znacznie wyższe niż w sytuacji, gdy mamy do czynienia z system o niskim wpływie na działalność biznesową, dla którego można wdrożyć mniej kosztowny system tworzenia kopii zapasowych. Wykreślenie punktów bilansu kosztów pokaże optymalny punkt między kosztem zakłócenia, a kosztami odzyskiwania. Punkt przecięcia (Punkt Bilansu Kosztów na Rysunku 3-3: Bilansowanie kosztów) będzie inny dla każdej organizacji i systemu, w zależności od ograniczeń finansowych i wymagań operacyjnych.

### 3.2.2 WYMAGANIA DOTYCZĄCE IDENTYFIKACJI ZASOBÓW

Realistyczne działania naprawcze wymagają dogłębnej oceny zasobów niezbędnych do jak najszybszego wznowienia procesów biznesowych. Współpracując z kierownictwem organizacji oraz wewnętrznymi i zewnętrznymi PoC związanymi z systemem, koordynator ISCP powinien dopilnować, aby zidentyfikowano kompletne zasoby systemu informatycznego. Proste zestawienie, takie jak pokazano w Tabeli 3-1, można wykorzystać

do przechowywania informacji o zasobach systemu informatycznego. W przypadku złożonych systemów informatycznych może być wymagana bardziej złożona metoda dokumentowania zasobów systemu.

**Tabela 3-1: Tabela zasobów / komponentów systemu informatycznego[6]**

| Zasób / komponent systemu | Platforma / system operacyjny / wersja (jeśli dotyczy) | Opis |
|---|---|---|
| *Serwer aplikacyjny* | *Sun V245/ Solaris / v10.0* | *Główny serwer aplikacyjny* |
| | | |
| | | |

### 3.2.3 OKREŚLANIE PRIORYTETÓW ODZYSKIWANIA ZASOBÓW SYSTEMOWYCH

Opracowanie priorytetów odzyskiwania jest ostatnim krokiem procesu BIA. Priorytety odzyskiwania można skutecznie ustalić, biorąc pod uwagę krytyczność procesu biznesowego, wpływ awarii, dopuszczalny czas przestoju i zasoby systemowe. Wynikiem jest hierarchia priorytetów odzyskiwania systemu informatycznego. Koordynator ISCP powinien rozważyć środki i technologie odzyskiwania systemu w celu spełnienia priorytetów odzyskiwania.

## 3.3 IDENTYFIKACJA ZABEZPIECZEŃ

W niektórych przypadkach skutki zakłócenia określone w BIA można złagodzić lub wyeliminować za pomocą środków zapobiegawczych, które uniemożliwiają, wykrywają lub ograniczają wpływ zakłócenia na system. Tam, gdzie jest to wykonalne i opłacalne, preferowane są metody zapobiegawcze niż działania, które mogą być konieczne do odzyskania systemu po zakłóceniu. Krok 2 RMF obejmuje identyfikację skutecznych zabezpieczeń prewencyjnych planowania awaryjnego i utrzymanie tych kontroli na bieżąco.

[6] Przykładowy zasób i platforma z opisem.

W NSC 800-53 zidentyfikowano różne zabezpieczenia, w zależności od typu systemu i konfiguracji. Niektóre typowe środki są wymienione poniżej:

- Zasilacze bezprzerwowe o odpowiedniej wydajności, zapewniające krótkoterminowe zasilanie rezerwowe dla wszystkich elementów systemu (w tym kontroli środowiska i bezpieczeństwa);
- Agregaty prądotwórcze, zapewniające długoterminowe zasilanie rezerwowe;
- Systemy klimatyzacji o odpowiedniej nadwyżce wydajności, aby zniwelować wpływ awarii niektórych elementów, takich jak np. pojedyncza sprężarka;
- Systemy przeciwpożarowe;
- Czujniki ognia i dymu;
- Czujniki wody na suficie i na podłodze / pod podłogą sali komputerowej;
- Odporne na ciepło i wodoodporne pojemniki na nośniki kopii zapasowych i niezbędne zapisy nieelektroniczne;
- Przeciwpożarowy wyłącznik awaryjny systemu zasilania;
- Zewnętrzne przechowywanie nośników kopii zapasowych, zapisów nieelektronicznych i dokumentacji systemowej;
- Zabezpieczenia techniczne, takie jak zarządzanie kluczami kryptograficznymi;
- Częste wykonywanie kopii zapasowych, w tym określenie miejsca przechowywania kopii zapasowych (lokalnie lub poza lokalizacją systemu) oraz plan ich rotacji i przenoszenia do magazynu.

## 3.4 TWORZENIE STRATEGII AWARYJNEJ

W organizacjach wymagane jest dążenie do odpowiedniego ograniczania ryzyka podczas realizacji procesów biznesowych, związanego z przetwarzaniem informacji w systemach informatycznych. Wyzwaniem dla organizacji jest wdrożenie odpowiedniego zestawu zabezpieczeń. W ramach RMF i zgodnie z NSC 199 i NSC 800-53 są dobierane i wdrażane

niezbędne zabezpieczenia. Strategie awaryjne tworzone są w celu zmniejszenia ryzyka w ramach całej rodziny planów awaryjnych i obejmują pełen zakres tworzenia kopii zapasowych, odzyskiwania, planowania awaryjnego, testowania i bieżącego utrzymania.

### 3.4.1 KOPIE ZAPASOWE I ODZYSKIWANIE

Metody i strategie tworzenia kopii zapasowych oraz odzyskiwania są sposobem na szybkie i skuteczne przywrócenie działania systemu po zakłóceniu działania usługi. Metody i strategie powinny uwzględniać wpływ zakłóceń i dopuszczalne przestoje zidentyfikowane w BIA i powinny być zintegrowane z architekturą systemu podczas fazy SDLC rozwoju lub pozyskania. Można rozważyć wiele różnych podejść do odzyskiwania, przy czym właściwy wybór będzie w dużym stopniu zależny od zakłócenia, rodzaju systemu, poziomu wpływu BIA / NSC 199 i wymagań operacyjnych systemu. Szczególne metody odzyskiwania, opisane dalej w sekcji 3.4.2, powinny podlegać rozważeniu i mogą obejmować umowy handlowe z dostawcami alternatywnych miejsc przetwarzania, umowy wzajemne (*ang. Reciprocal Agreements)* z organizacjami wewnętrznymi lub zewnętrznymi oraz umowy dotyczące gwarancji poziomu usług (SLA) z dostawcami sprzętu. Ponadto przy opracowywaniu strategii odzyskiwania systemu należy wziąć pod uwagę technologie, takie jak nadmiarowe macierze niezależnych dysków (RAID), automatyczne przełączanie awaryjne, UPS, klastrowanie serwerów i systemy lustrzane.

Opracowując i porównując strategie, należy wziąć pod uwagę kilka alternatywnych podejść, w tym koszty, maksymalne przestoje, bezpieczeństwo, priorytety odzyskiwania oraz integrację z większymi planami awaryjnymi na poziomie organizacji. Tabela jest przykładem, który może pomóc w identyfikacji powiązania poziomu wpływu NSC 199 dla atrybutu bezpieczeństwa w postaci dostępności, priorytetu odzyskiwania, kopii zapasowej i strategii odzyskiwania.

**Tabela 3-2: Przykładowa analiza wg. NSC 199 dla kategorii Kopie zapasowe i Odzyskiwanie**

| Poziom wpływu zakłócenia na dostępność wg NSC 199 | Priorytet systemu informatycznego w zakresie odzyskiwania | Strategia kopi zapasowych i odzyskiwania |
|---|---|---|
| **Niski** | Priorytet niski - jakakolwiek awaria ma niewielki wpływ na szkody lub zakłócenia działania organizacji. | Kopia zapasowa: kopia zapasowa na taśmach lub innym nośniku.<br>Strategia: przeniesienie przetwarzania lub zimna rezerwa (zapasowe miejsce przetwarzania). |
| **Umiarkowany** | Priorytet istotny lub umiarkowany - każdy, który w przypadku zakłócenia spowodowałby umiarkowany problem dla organizacji i ewentualnie innych sieci lub systemów. | Kopia zapasowa: kopia na nośniku optycznym, replikacja WAN / VLAN.<br>Strategia: zimna lub gorąca rezerwa (zapasowe miejsce przetwarzania). |
| **Wysoki** | Priorytet krytyczny lub wysoki - uszkodzenie lub zakłócenie działania tych systemów wywarłoby największy wpływ na organizację i jej cel działania oraz na inne sieci i systemy. | Kopia zapasowa: systemy lustrzane i replikacja dysków on-line.<br>Strategia: gorąca rezerwa (zapasowe miejsce przetwarzania). |

### 3.4.2 METODY TWORZENIA KOPII ZAPASOWYCH I PRZECHOWYWANIE POZA SIEDZIBĄ ORGANIZACJI

Dane systemowe powinny być regularnie przenoszone do kopii zapasowych. W oparciu o krytyczność danych i częstotliwość wprowadzania nowych informacji, powinny zostać określone zasady tworzenia kopii zapasowych obejmujące minimalną częstotliwość tworzenia kopii zapasowych i ich zakres (np. dzienna lub tygodniowa, przyrostowa lub pełna). Zasady tworzenia kopii zapasowych danych powinny określać lokalizację przechowywanych danych, konwencje nazewnictwa plików, częstotliwość rotacji nośników oraz metodę transportu danych poza miejsce. Kopię zapasową danych można wykonać na dysku magnetycznym, taśmie lub dyskach optycznych. Konkretna metoda wybrana do wykonywania kopii zapasowych powinna opierać się na wymaganiach dotyczących dostępności i integralności systemu i danych. Metody te mogą obejmować systemy skarbca elektronicznego, pamięci sieciowej i bibliotek taśmowych.

Dobrą praktyką biznesową jest przechowywanie kopii zapasowych danych poza siedzibą firmy. Komercyjne urządzenia do przechowywania danych są specjalnie zaprojektowane do archiwizowania mediów i ochrony danych przed zagrożeniami. Jeśli organizacja korzysta z pamięci zewnętrznej, dane są kopiowane w obiekcie organizacji, a następnie etykietowane, pakowane i transportowane do magazynu. Jeśli dane są wymagane do celów odzyskiwania lub testowania, organizacja kontaktuje się z magazynem z prośbą o przesłanie określonych danych do organizacji lub do alternatywnego obiektu. Przy wyborze zewnętrznego magazynu i dostawcy należy wziąć pod uwagę następujące kryteria:

- Obszar geograficzny: odległość od organizacji i prawdopodobieństwo, że miejsce przechowywania zostanie dotknięte tą samą katastrofą, co główna siedziba organizacji;
- Dostępność: czas niezbędny do odzyskania danych z pamięci oraz godziny pracy magazynu;

- Bezpieczeństwo: metod transportu, obiektu służącego do przechowywania i personelu; wszystkie one muszą spełniać zakładane przez organizację wymogi bezpieczeństwa danych;
- Środowisko: warunki strukturalne i środowiskowe obiektu magazynowego (tj. temperatura, wilgotność, zapobieganie pożarom i sterowanie zarządzania energią);
- Koszt: koszt wysyłki, opłaty operacyjne oraz usługi reagowania / odzyskiwania po awarii.

### 3.4.3 ZAPASOWE MIEJSCA PRZETWARZANIA

Kategoryzacja bezpieczeństwa NSC 199 dla atrybutu bezpieczeństwa jakim jest dostępność określa, które mechanizmy zabezpieczeń mają zastosowanie do konkretnego systemu. Na przykład system informacyjny sklasyfikowany jako posiadający atrybut niskim wpływie zakłócenia nie wymaga alternatywnej pamięci masowej ani alternatywnego miejsca przetwarzania (odpowiednio CP-6 i CP-7)[7], a system informatyczny posiadający atrybut bezpieczeństwa umiarkowanego wpływu zakłócenia wymaga kopii zapasowej systemu i testowanie tej kopii (CP-9 [1])[8]. Dalsze szczegóły i opisy zabezpieczeń planowania awaryjnego znajdują się w załączniku E.

Chociaż poważne zakłócenia o długofalowych skutkach mogą być rzadkie, należy je uwzględnić w planie awaryjnym. Zatem dla wszystkich systemów o umiarkowanym lub dużym wpływie zakłócenia, plan powinien obejmować strategię odzyskiwania i wykonywania operacji systemowych w alternatywnym obiekcie przez dłuższy okres. Organizacje mogą rozważyć przeniesienie systemu o niskim wpływie zakłócenia do alternatywnego miejsca przetwarzanie danych, ale jest to decyzja organizacyjna i nie jest wymagana. Zasadniczo dostępne są trzy typy alternatywnych miejsc przetwarzania:

[7] Zabezpieczenia CP-6 i CP-7 dokumentu NSC 800-53.
[8] Zabezpieczenie rozszerzone nr 1 katalogu zabezpieczeń CP-9 dokumentu NSC 800-53.

- Dedykowane miejsce przetwarzania będące własnością organizacji lub zarządzane przez nią;
- Wzajemna umowa lub porozumienie różnymi organizacjami;
- Obiekt wynajęty komercyjnie.

Bez względu na rodzaj wybranego alternatywnego miejsca przetwarzania, obiekt musi być w stanie wspierać operacje systemowe określone w planie awaryjnym. Pod względem gotowości operacyjnej wyróżnia się trzy alternatywne typy zapasowych miejsc przetwarzania, klasyfikowane jako zapasowe miejsca przetwarzania: *zimne, ciepłe lub gorące*. Mogą występować inne odmiany klasyfikacji lub ich kombinacje, ale generalnie wszystkie odmiany zachowują podobne funkcje podstawowe występujące w jednym z tych trzech typów zapasowych miejsc przetwarzania. Poniżej opisano typy zapasowych miejsc przetwarzania, przechodząc od podstawowego do zaawansowanego.

- **Typ zimny** – to zazwyczaj obiekty z odpowiednią przestrzenią i infrastrukturą (energia elektryczna, połączenia telekomunikacyjne i zabezpieczenia środowiskowe) służące do wspierania działań związanych z odzyskiwaniem systemu informatycznego (brak zainstalowanego na stałe sprzętu teleinformatycznego).
- **Typ ciepły** – to obiekty częściowo wyposażone, które zawierają część lub całość sprzętu systemowego, oprogramowania, telekomunikacji i źródeł zasilania.
- **Typ gorący** – to obiekty odpowiednio przygotowane do wymagań systemowych i skonfigurowane w niezbędny sprzęt systemowym, infrastrukturę wspierającą i personelem wsparcia.

Jak omówiono powyżej, najczęściej występują wspomniane trzy alternatywne typy zapasowych miejsc przetwarzania. Istnieją również ich odmiany posiadające mieszanki cech. Każda organizacja powinna ocenić swoje podstawowe wymagania w celu ustalenia najbardziej skutecznego rozwiązania. Dwa przykłady odmian typów zapasowych miejsc przetwarzania to:

- Mobilne zapasowe miejsca przetwarzania, które są niezależnymi, przenośnymi kontenerami dostosowanymi do konkretnego sprzętu telekomunikacyjnego i systemowego niezbędnego do spełnienia wymagań systemowych.
- Lustrzane zapasowe miejsca przetwarzania, które są rozwiązaniami w pełni redundantnymi, z automatycznym dublowaniem informacji w czasie rzeczywistym. Lustrzane zapasowe miejsca przetwarzania są identyczne z lokalizacją główną pod każdym względem technicznym i są wzajemnie zastępowalne.

Istnieją oczywiste różnice w kosztach i czasie gotowości między opcjami. W wymienionych powyżej przykładach lustrzane miejsce przetwarzania jest najdroższym wyborem, ale zapewnia praktycznie 100-procentową dostępność. Zimne miejsca są najtańsze w utrzymaniu, chociaż mogą wymagać znacznego czasu na zakup i instalację niezbędnego sprzętu. Częściowo wyposażone miejsca, takie jak miejsca ciepłe, mieszczą się w środku spektrum. W wielu przypadkach miejsca mobilne mogą zostać dostarczone do wybranej lokalizacji w ciągu 24 godzin, ale czas niezbędny do instalacji i konfiguracji sprzętu może wydłużyć osiągnięcie gotowości do pracy. Wybór nowej lokalizacji powinien uwzględniać czas i rodzaj transportu niezbędny do przeniesienia tam personelu i sprzętu. Ponadto ustalone miejsce powinno znajdować się w obszarze geograficznym, na który prawdopodobnie nie będzie miało negatywnego wpływu to samo zagrożenie, co na główne miejsce przetwarzania.

Poniższa tabela podsumowuje kryteria, które można zastosować, aby określić, który typ alternatywnego miejsca przetwarzania spełnia wymagania organizacji. Miejsca przetwarzania powinny być analizowane przez organizację, biorąc pod uwagę wpływ na biznes i przestoje określone w BIA. Podczas oceny miejsca przetwarzania, koordynator ISCP powinien upewnić się, że bezpieczeństwo systemu, zarządzanie, zabezpieczenia organizacyjne i techniczne dla danego miejsca są zgodne z wymaganiami organizacji. Przykładowo, takie zabezpieczenia mogą obejmować zapory sieciowe, fizyczną kontrolę dostępu oraz wymagania dotyczące bezpieczeństwa personelu obsługującego miejsce przetwarzania.

**Tabela 3-3: Przykładowe kryteria zapasowych miejsc przetwarzania**

| Typ zapasowego miejsca przetwarzania | Koszt | Wyposażenie sprzętowe | Wyposażenie telekomunikacyjne | Czas konfiguracji | Lokalizacja |
|---|---|---|---|---|---|
| **Zimne** | niski | brak | brak | długi | stała |
| **Ciepłe** | średni | częściowe | częściowe/pełne | średni | stała |
| **Gorące** | średni/ wysoki | pełne | pełne | krótki | stała |

Zapasowe miejsca przetwarzania mogą być własnością organizacji i być przez nią obsługiwane (odzyskiwanie wewnętrzne) lub mogą być dostępne komercyjnie, na podstawie zawartej umowy. W przypadku zawarcia umowy na zapasowe miejsce pracy z dostawcą komercyjnym, należy wynegocjować odpowiedni czas na testowanie, przestrzeń roboczą, wymagania bezpieczeństwa, wymagania sprzętowe, wymagania telekomunikacyjne, usługi wsparcia i okres odzyskiwania (jak długo organizacja może zajmować miejsce zapasowe w okresie odzyskiwania) i wyraźnie określić to w umowie. Klienci powinni mieć świadomość, że wiele organizacji może zawrzeć umowę ze sprzedawcą tego samego zapasowego miejsca przetwarzania wielu innym klientom. W rezultacie miejsce może nie być w stanie pomieścić wszystkich klientów, jeśli katastrofa dotknie dużą liczbę tych klientów jednocześnie. Należy wynegocjować zasady kupna / sprzedaży dotyczące sposobu rozwiązania tej sytuacji i ustalenia statusu priorytetu, który otrzyma dana organizacja.

Dwie lub więcej organizacji z podobnymi lub identycznymi konfiguracjami systemów i technologiami tworzenia kopii zapasowych może zawrzeć formalną umowę, która ma służyć jako alternatywne lokalizacje dla każdej z nich lub zawrzeć wspólną umowę dla alternatywnej lokalizacji. Taki typ zapasowych miejsc pracy jest konfigurowany na podstawie wzajemnej umowy lub protokołu ustaleń (*ang. memorandum of understanding -MoU*).

Wzajemne porozumienie należy zawrzeć ostrożnie, ponieważ każde z miejsc w przypadku awarii oprócz własnego obciążenia musi być w stanie obsługiwać również drugą organizację. Ten rodzaj umowy wymaga, aby sekwencje odzyskiwania systemów z obu organizacji były traktowane priorytetowo ze wspólnej perspektywy, korzystnej dla obu stron. W lokalizacjach partnerskich należy przeprowadzić testy w celu oceny dodatkowych progów wydajności przetwarzania, zgodności konfiguracji systemu i kopii zapasowych, przepustowości połączeń telekomunikacyjnych, kompatybilności środków bezpieczeństwa oraz wrażliwości danych, które mogą być dostępne dla uprzywilejowanych użytkowników drugiej organizacji. Należy również wziąć pod uwagę wzajemne połączenia systemowe i ewentualne umowy o bezpiecznym połączeniu systemów (ISA).

Dla alternatywnego miejsca przetwarzania należy opracować protokół ustaleń (MoU) lub umowę SLA, dostosowane do potrzeb danej organizacji i możliwości organizacji partnerskiej. Dział prawny każdej ze stron musi przejrzeć i zatwierdzić umowę. Zasadniczo umowa powinna obejmować co najmniej następujące elementy:

- Czas trwania umowy;
- Strukturę wszystkich kosztów oraz harmonogramy fakturowania i płatności;
- Definicje awarii (tj. okoliczności stanowiące awarię, procedury powiadamiania);
- Priorytet dostępu do miejsca przetwarzania;
- Dostępność miejsca;
- Gwarancja odnoszące się do miejsca;
- Wskazanie istnienia innych klientów współużytkujących te same zasoby miejsca oraz całkowitą liczba subskrybentów miejsca, jeśli dotyczy;
- Proces zmiany lub modyfikacji umowy;
- Warunki rozwiązania umowy;
- Proces negocjowania rozszerzenia usługi;
- Gwarancję zgodności;

- Wymagania systemu informatycznego (w tym wymagania dotyczące danych i telekomunikacji) dotyczące sprzętu, oprogramowania oraz wszelkich specjalnych potrzeb systemowych (sprzęt i oprogramowanie);
- Zarządzanie zmianą i powiadamianie, w odniesieniu do sprzętu, oprogramowania i infrastruktury;
- Wymagania bezpieczeństwa, w tym specjalne potrzeby w zakresie bezpieczeństwa;
- Zapewnienie lub nie zapewnienie wsparcie personelu i zakres tego wsparcia;
- Możliwość korzystania z dodatkowych usług świadczonych w danym miejscu (korzystanie ze sprzętu biurowego, parkingów, stołówki itp.);
- Zasady testowania, w tym planowanie, dostępność, czas trwania testu i dodatkowe testy, jeśli jest to wymagane;
- Zarządzanie dokumentacją (na miejscu i poza siedzibą), w tym na nośnikach elektronicznych i wydrukach;
- Zarządzanie na poziomie usług (pomiary wydajności i zarządzanie jakością świadczonych usług systemu informatycznego);
- Wymagania dotyczące miejsca do pracy (np. krzesła, biurka, telefony, komputery osobiste);
- Zaopatrzenie w materiały eksploatacyjne (np. artykuły biurowe);
- Dodatkowe koszty nie pokryte gdzie indziej;
- Inne kwestie dotyczące umowy, w stosownych przypadkach;
- Inne wymagania techniczne, w stosownych przypadkach.

### 3.4.4 WYMIANA WYPOSAŻENIA

Jeśli system informacyjny zostanie uszkodzony lub zniszczony lub główne miejsce przetwarzania będzie niedostępne, zachodzi potrzeba szybkiego aktywowania lub zakupienia sprzętu i oprogramowania i dostarczenia ich do innej lokalizacji. Istnieją trzy podstawowe strategie przygotowania do wymiany sprzętu.

- **Umowy z dostawcami**. W trakcie opracowywania planu awaryjnego mogą zostać zawarte umowy SLA z dostawcami sprzętu, oprogramowania i usług wsparcia technicznego. Umowa SLA powinna określać, jak szybko dostawca musi odpowiedzieć po otrzymaniu powiadomienia. Umowa powinna również nadać organizacji priorytetowy status w zakresie transportu sprzętu zastępczego w stosunku do sprzętu zakupionego do normalnych operacji. Umowa SLA powinna także określać, jaki status priorytetowy otrzyma organizacja w przypadku katastrofy z udziałem wielu klientów. W takich przypadkach organizacje z procesami od których zależy zdrowie i bezpieczeństwo, często otrzymają najwyższy priorytet. Szczegóły tych negocjacji powinny zostać udokumentowane w umowie SLA, którą należy zachować wraz z planem awaryjnym.
- **Magazynowanie sprzętu.** Wymagany sprzęt można kupić z wyprzedzeniem i przechowywać w bezpiecznym miejscu poza siedzibą, na przykład w zapasowym miejscu przetwarzania, w którym odbywać się będą operacje odzyskiwania (miejsce ciepłe lub mobilne) albo w innym miejscu, w którym będą przechowywane, a następnie wysłane do właściwego miejsca. To rozwiązanie ma pewne wady. Organizacja musi przeznaczyć środki finansowe na zakup tego sprzętu z wyprzedzeniem, a sprzęt może z czasem stać się przestarzały lub nieodpowiedni do użytku z powodu zmian technologii i wymagań systemowych.
- **Istniejące urządzenia kompatybilne**. Do odtwarzania awaryjnego wykorzystywany będzie sprzęt i oprogramowanie znajdujące się w gorącym zapasowym miejscu przetwarzania. Obejmuje to też umowy wzajemnego zapewnienia zapasowych miejsc przetwarzania.

Oceniając wybory, koordynator ISCP powinien wziąć pod uwagę, że zakup sprzętu w razie wystąpienia potrzeby jest opłacalny, ale może wydłużyć czas potrzebny na odzyskanie z powodu oczekiwania na wysyłkę i konfigurację. Odwrotnie, przechowywanie nieużywanego sprzętu jest kosztowne, ale umożliwia szybsze rozpoczęcie operacji odzyskiwania. Wybierając najbardziej odpowiednią strategię, należy pamiętać, że dostępność transportu może być ograniczona lub czasowo wstrzymana w przypadku rozległej katastrofy. W oparciu o skutki uwidocznione za pośrednictwem analizy BIA, należy wziąć pod uwagę możliwość powszechnej katastrofy obejmującej masową wymianę sprzętu i opóźnienia transportu, które przedłużyłyby okres odzyskiwania. Niezależnie od wybranej strategii, szczegółowe plany potrzeb i specyfikacji sprzętu powinny być przechowywane w ramach planu awaryjnego. Dodatkowo należy uwzględnić, czy dany sprzęt znajduje się w powszechnej sprzedaży, czy też wykonywany jest na jednostkowe zamówienie. Dokumentacja wykazu urządzeń została omówiona dalej w rozdziale 4.1.

### 3.4.5 UWAGI DOTYCZĄCE KOSZTÓW

Koordynator ISCP powinien upewnić się, że wybraną strategię można skutecznie wdrożyć przy użyciu dostępnego personelu i posiadanych zasobach finansowych. Koszt każdego rozważanego zapasowego miejsca przetwarzania, wymiany sprzętu i opcji przechowywania należy porównać z ograniczeniami budżetowymi. Koordynator powinien określić znane wydatki na planowanie awaryjne, takie jak opłaty za alternatywne kontrakty na zapasowe miejsce przetwarzania oraz te, które są mniej oczywiste, takie jak koszt wdrożenia programu świadomości awaryjnej obejmującego całą organizację i wsparcie wykonawcy. Budżet musi być wystarczający na pokrycie oprogramowania, sprzętu, podróży i wysyłki, testowania, planowania programów szkoleniowych, programów uświadamiających, godzin pracy personelu, innych zleconych usług oraz wszelkich innych odpowiednich zasobów (np. biurka, telefony, faksy, długopisy i papier). Organizacja powinna przeprowadzić analizę kosztów i korzyści w celu zidentyfikowania optymalnej strategii awaryjnej. Tabela zawiera szablon do oceny kwestii kosztowych.

**Tabela 3-4: Szablon planowania budżetu strategii awaryjnej**

| Zasoby planu awaryjnego | Strategie | Koszty dostawcy | Koszty sprzętu | Koszty oprogramowania | Koszty transportu | Koszty pracy lub usług | Koszty testowania | Koszty zaopatrzenia |
|---|---|---|---|---|---|---|---|---|
| **Zapasowe miejsce przetwarzania** | Miejsce zimne | | | | | | | |
| | Miejsce ciepłe | | | | | | | |
| | miejsce gorące | | | | | | | |
| **Przechowywanie poza siedzibą organizacji** | Komercyjne | | | | | | | |
| | Wewnętrzne | | | | | | | |
| **Wymiana sprzętu** | SLA | | | | | | | |
| | Magazynowanie | | | | | | | |
| | Użycie posiadanych zasobów | | | | | | | |

### 3.4.6 ROLE I ODPOWIEDZIALNOŚĆ

Po wybraniu i wdrożeniu strategii tworzenia kopii zapasowych i odzyskiwania systemu, koordynator ISCP musi wyznaczyć odpowiednie zespoły do wdrożenia strategii. Każdy zespół powinien zostać przeszkolony i być gotowy do reagowania w przypadku zakłócenia wymagającego aktywacji planu. Personel ds. odzyskiwania powinien zostać przypisany do jednego z kilku konkretnych zespołów, które zareagują na zdarzenie, odzyskają możliwości i przywrócą system do normalnej pracy. Aby to zrobić, członkowie zespołu odzyskiwania muszą jasno zrozumieć cel wysiłku odzyskiwania, poszczególne procedury, które zespół

wykona oraz to, w jaki sposób współzależności między zespołami odzyskiwania mogą wpłynąć na ogólne strategie.

Wymagane typy zespołów zależą od systemu informatycznego, którego dotyczy problem i można je dostosować zgodnie z poziomami wpływu NSC 199, aby odzwierciedlić określone różnice w wymaganiach i procedurach tworzenia kopii zapasowych. Rozmiar każdego zespołu, nazwy zespołów i projekty hierarchii zależą od organizacji. Oprócz pojedynczej autorytatywnej roli w zakresie ogólnej odpowiedzialności za podejmowanie decyzji, w tym aktywacji planu, skuteczna strategia będzie wymagać niektórych lub wszystkich następujących grup:

- Zespół zarządzający (w tym koordynator ISCP);
- Zespół oceny awarii;
- Zespół administracji systemu operacyjnego;
- Zespół odzyskiwania serwera (np. serwer klienta, serwer WWW);
- Zespół odzyskiwania sieci lokalnej / sieci rozległej (LAN / WAN);
- Zespół odzyskiwania bazy danych;
- Zespół odzyskiwania operacji sieciowych;
- Zespół (y) odzyskiwania aplikacji;
- Zespół telekomunikacyjny;
- Zespół testowy;
- Zespół transportu i relokacji;
- Zespół ds. relacji z mediami;
- Zespół ds. prawnych;
- Zespół ochrony fizycznej / personelu;
- Zespół zaopatrzenia (sprzęt i materiały).

Należy dobrać personel do obsługi tych zespołów w oparciu o ich umiejętności i posiadaną wiedzę. Zespoły powinny się składać z personelu odpowiedzialnego za te same lub podobne funkcje w normalnych warunkach. Na przykład członkami zespołu odzyskiwania serwera powinni być administratorzy tego serwera. Członkowie zespołu muszą zrozumieć nie tylko cel planu awaryjnego, ale także procedury niezbędne do wykonania strategii odzyskiwania. Zespoły powinny mieć wystarczającą wielkość, aby zachować rentowność. Jeśli niektórzy członkowie nie są w stanie wziąć udziału w danym zespole, należy wyznaczyć zastępców członków zespołu. Członkowie zespołu powinni znać cele i procedury innych zespołów, aby ułatwić koordynację między zespołami. Koordynator ISCP powinien również wziąć pod uwagę, że zakłócenie może uniemożliwić niektórym pracownikom wzięcie udziału w planie awaryjnym (np. na zachorowania podczas epidemii). W tej sytuacji realizacja planu może być możliwa tylko przy użyciu personelu z innego obszaru geograficznego organizacji lub poprzez zatrudnienie kontrahentów lub dostawców. Taki personel powinien być koordynowany i szkolony jako zespół zastępczy.

Każdy zespół jest zarządzany przez lidera zespołu, który kieruje ogólnymi działaniami zespołu, działa jako przedstawiciel zespołu na poziomie zarządzania i współpracuje z innymi liderami zespołu. Lider zespołu rozpowszechnia informacje wśród członków zespołu i zatwierdza wszelkie decyzje, które należy podjąć w zespole. Lider zespołu powinien mieć wyznaczonego zastępcę, który będzie działać jako menadżer, jeśli główny lider jest niedostępny. W przypadku większości systemów, zespół zarządzający jest niezbędny do zapewnienia ogólnych wskazówek w przypadku poważnej awarii systemu. Zespół jest odpowiedzialny za aktywację planu awaryjnego i nadzór nad realizacją operacji awaryjnych. Zespół zarządzający ułatwia również komunikację między innymi zespołami, nadzoruje testy i ćwiczenia planu awaryjnego systemu informatycznego. Część lub cały zespół zarządzający może kierować wyspecjalizowanymi zespołami ds. odzyskiwania. Funkcja / rola, taka jak CIO, stanowi najwyższy organ w aktywacji planu i podejmowaniu decyzji dotyczących poziomów wydatków, akceptowalnego ryzyka i koordynacji międzyorganizacyjnej. Wyższy menadżer zarządzający zazwyczaj kieruje zespołem zarządzającym.

## 3.5 PLANOWANIE TESTÓW, SZKOLEŃ I ĆWICZEŃ (TT&E)

ISCP należy utrzymywać w stanie gotowości, który obejmuje przeszkolenie personelu w zakresie wypełniania jego ról i obowiązków w ramach planu, wykonywanie planów w celu weryfikacji ich treści oraz testowanie systemów i komponentów systemu w celu zapewnienia ich operacyjności w środowisku określonym w ISCP. Ponadto, jak wskazano w kroku 4 (Ocena zabezpieczeń) RMF, skuteczność kontroli systemu informatycznego należy oceniać, stosując procedury udokumentowane w NSC 800-53 – Zasady stosowania zabezpieczeń w systemach informatycznych podmiotów publicznych. Aby organizacje mogły poprawić swoją zdolność do przygotowania się na zdarzenia niepożądane, reagować na nie, zarządzać nimi i odzyskać zdolność do działania, plany awaryjne muszą być testowane, a personel powinien podlegać szkoleniom i brać udział w ćwiczeniach. Chociaż większość działań związanych z TT&E (*ang. Plan Testing, Training, and Exercises* ) ma miejsce podczas fazy operacji / utrzymania, początkowe zdarzenia TT&E należy przeprowadzić podczas fazy wdrażania / oceny SDLC, aby potwierdzić procedury odzyskiwania ISCP.

Organizacje powinny przeprowadzać wydarzenia związane z TT&E okresowo, po zmianach organizacyjnych lub systemowych, wydaniu nowych wytycznych dotyczących TT&E lub w razie innej potrzeby. Realizacja wydarzeń TT&E pomaga organizacjom w określeniu skuteczności planu oraz zapewnia, że wszyscy pracownicy wiedzą, jakie są ich role w realizacji każdego planu dla konkretnego systemu informatycznego. Harmonogramy wydarzeń TT&E są często częściowo podyktowane wymogami organizacyjnymi. Na przykład NSC 800-53 obejmuje zabezpieczenie (CP-4) stanowiące o potrzebie przeprowadzania ćwiczeń lub testów planów awaryjnych w odniesieniu do systemów z częstotliwością określoną przez organizację. Sekcja 3.5.4 zawiera wytyczne dotyczące rodzaju TT&E zidentyfikowanych dla każdego poziomu wpływu zakłócenia określonego w NSC 199.

Dla każdej przeprowadzonej czynności TT&E jej wyniki są dokumentowane w stosownym raporcie, a działania korygujące wyciągnięte z wniosków są rejestrowane w celu aktualizacji informacji w ISCP.

### 3.5.1 TESTOWANIE

Testowanie ISCP jest kluczowym elementem realnej zdolności awaryjnej. Testowanie umożliwia identyfikację i usunięcie braków w planie poprzez sprawdzenie jednego lub więcej elementów systemu i operacyjności planu. Testy mogą przybierać różne formy i osiągać kilka celów, ale powinny być przeprowadzane w możliwie adekwatnym otoczeniu operacyjnym. Każdy element systemu informatycznego powinien zostać przetestowany w celu potwierdzenia dokładności poszczególnych procedur odzyskiwania. W ramach testu planu awaryjnego należy odpowiednio uwzględnić następujące obszary:

- Procedury powiadamiania;
- Odzyskiwanie systemu na alternatywnej platformie z nośnika kopii zapasowej;
- Łączność wewnętrzna i zewnętrzna;
- Wydajność systemu przy użyciu alternatywnego sprzętu;
- Przywrócenie normalnej pracy;
- Inne testy planu (w przypadku zidentyfikowania koordynacji, tj. COOP, BCP).

Aby osiągnąć jak największą korzyść z testu, koordynator ISCP powinien opracować plan testów zaprojektowany w celu zbadania wybranych elementów na podstawie jednoznacznych celów testu i kryteriów sukcesu. Zastosowanie celów testu i kryteriów sukcesu umożliwia ocenę skuteczności każdego elementu systemu i ogólnego planu. Plan testów powinien zawierać harmonogram wyszczególniający ramy czasowe każdego testu i uczestników testu. Plan testów powinien również wyraźnie określać zakres, scenariusz i logistykę. Wybrany scenariusz może być najgorszym przypadkiem lub najbardziej prawdopodobnym zdarzeniem. Powinien naśladować rzeczywistość tak dokładnie, jak to możliwe.

| | |
|---|---|
| ***Testowanie*** | *Testy są narzędziami oceniającymi, które wykorzystują kwantyfikowalne wskaźniki do sprawdzania poprawności działania systemu informatycznego lub komponentu systemu w środowisku operacyjnym. Na przykład organizacja może przetestować listy drzew połączeń, aby ustalić, czy można wykonać połączenie w wyznaczonym terminie; innym testem może być odłączenie zasilania od systemu lub elementu systemu. Test przeprowadza się w możliwie adekwatnym środowisku operacyjnym; jeżeli jest to wykonalne, należy zastosować faktyczny test komponentów lub systemów używanych do prowadzenia codziennych operacji w organizacji. Zakres testów może obejmować różne komponenty lub systemy do kompleksowych testów wszystkich systemów i komponentów obsługiwanych przez ISCP. Testy często koncentrują się na operacjach odzyskiwania i tworzenia kopii zapasowych; jednak testy różnią się w zależności od poziomu wpływu NSC 199, celu testu i jego związku z konkretnym ISCP.* |

### 3.5.2 SZKOLENIE

Szkolenie personelu w zakresie obowiązków związanych z planem awaryjnym powinno koncentrować się na zapoznaniu ich z rolami w ISCP i nauczaniu umiejętności niezbędnych do pełnienia tych ról. Takie podejście pomaga przygotować pracowników do uczestnictwa w testach i ćwiczeniach, a także faktycznych zdarzeniach awaryjnych. Szkolenie powinno odbywać się co najmniej raz w roku. Personel nowo wyznaczony na stanowiska w ISCP powinien przejść szkolenie tak szybko, jak to możliwe. Docelowo personel ISCP powinien zostać przeszkolony tak, aby był w stanie wykonywać swoje role i obowiązki związane z odzyskiwaniem bez pomocy dokumentacji ISCP. Jest to ważny cel w przypadku, gdy papierowe lub elektroniczne wersje planu, w wyniku zakłócenia, będą niedostępne przez pierwsze kilka godzin. Personel zajmujący się odzyskiwaniem powinien zostać przeszkolony w zakresie następujących elementów planu:

- Cel planu;

- Koordynacja i komunikacja między zespołami;
- Procedury sprawozdawcze;
- Wymagania bezpieczeństwa;
- Procesy specyficzne dla zespołu (fazy aktywacji i powiadomień, odzyskiwania i odtwarzania);
- Indywidualne obowiązki (aktywacja i powiadomienie, odzyskiwanie i odtwarzanie).

| | |
|---|---|
| ***Szkolenie*** | *Dla celów niniejszej publikacji, szkolenie dotyczy jedynie informowania personelu o jego rolach i obowiązkach w ramach konkretnego planu systemu informatycznego oraz uczenia ich umiejętności związanych z tymi rolami i obowiązkami, przygotowując ich do uczestnictwa w ćwiczeniach, testach i rzeczywistych sytuacjach awaryjnych związanych z ISCP. Szkolenie personelu w zakresie jego ról i obowiązków przed ćwiczeniem lub testem, jest zwykle podzielone na prezentację dotyczącą ich ról i obowiązków oraz działania, które pozwalają personelowi wykazać się zrozumieniem przedmiotu tych działań.* |

### 3.5.3 ĆWICZENIA

Zwykle określa się następujące rodzaje ćwiczeń szeroko stosowane w programach TT&E w systemie informatycznym przez poszczególne organizacje:

- **Ćwiczenia aplikacyjne.** Ćwiczenia aplikacyjne są ćwiczeniami opartymi na dyskusjach, podczas których personel spotyka się w pomieszczeniu szkoleniowym lub w grupach grup dyskusyjnych, aby omówić swoje role podczas zagrożenia i ich reakcje na określoną sytuację awaryjną. Prowadzący ćwiczenia przedstawia scenariusz i zadaje uczestnikom ćwiczenia pytania związane ze scenariuszem, co inicjuje dyskusję między uczestnikami na temat ról, obowiązków, koordynacji i podejmowania decyzji. Ćwiczenie aplikacyjne jest oparte wyłącznie na dyskusji i nie wymaga rozmieszczania sprzętu ani innych zasobów.

- **Ćwiczenia funkcjonalne.** Ćwiczenia funkcjonalne pozwalają personelowi zweryfikować gotowość operacyjną na wypadek awarii, poprzez wykonywanie swoich obowiązków w symulowanym środowisku operacyjnym. Ćwiczenia funkcjonalne są zaprojektowane tak, aby wykonywać role i obowiązki przez określonych członków zespołu, z użyciem procedur i zasobów zaangażowanych w jeden lub więcej funkcjonalnych aspektów planu (np. komunikacja, powiadomienia awaryjne, konfiguracja sprzętu systemowego). Ćwiczenia funkcjonalne różnią się złożonością i zakresem, od walidacji określonych aspektów w ramach planu do pełnowymiarowych ćwiczeń obejmujących wszystkie elementy planu. Ćwiczenia funkcjonalne pozwalają pracownikom wykonywać swoje role i obowiązki tak, jak w rzeczywistej sytuacji awaryjnej, ale w sposób symulowany.

| | |
|---|---|
| ***Ćwiczenia*** | *Ćwiczenie to symulacja sytuacji awaryjnej, mająca na celu sprawdzenie wykonalności jednego lub większej liczby aspektów ISCP. W ćwiczeniu pracownicy z określonymi rolami i obowiązkami w danym ISCP, spotykają się, aby zweryfikować treść planu poprzez omówienie swoich ról i reakcji na sytuacje kryzysowe, wykonanie działań w symulowanym środowisku operacyjnym lub poprzez inne środki sprawdzania poprawności reakcji, które nie wymagają korzystania z rzeczywistego środowiska operacyjnego. Ćwiczenia są oparte na scenariuszach, takich jak awaria zasilania w jednym z centrów przetwarzania danych organizacji lub pożar, który powoduje uszkodzenie niektórych systemów, a dodatkowe sytuacje często pojawiają się w trakcie ćwiczenia.* |

### 3.5.4 PODSUMOWANIE

Program TT&E zapewnia ogólne ramy dla określania, planowania i ustalania celów działań TT&E. Głębokość i rygor działań TT&E ISCP wzrasta wraz z atrybutem dostępności zgodnie z NSC 199. Wszystkie testy i ćwiczenia powinny zawierać określenie wpływu na działalność organizacji i zapewnić mechanizm aktualizacji i ulepszenia planu.

Każdy z trzech szablonów ISCP (niski, umiarkowany i wysoki wg. NSC 199) zawarty w dodatkach do niniejszego przewodnika, zawiera szczegółowe informacje na temat prowadzenia działań związanych z TT&E odpowiednio do ich poziomu wpływu.

- W przypadku systemów o niskim wpływie na działanie organizacji wystarczające jest ćwiczenie na stole z częstotliwością zdefiniowaną przez organizację. Założenie do ćwiczenia powinno symulować zakłócenie, obejmować wszystkie główne punkty kontaktowe ISCP i być przeprowadzany przez właściciela systemu lub inny odpowiedzialny organ.
- W przypadku systemów o umiarkowanym wpływie na działanie organizacji, należy przeprowadzić ćwiczenia funkcjonalne z częstotliwością określoną przez organizację. Ćwiczenie funkcjonalne powinno obejmować wszystkie punkty kontaktowe ISCP i powinno być umożliwione przez właściciela systemu lub odpowiedzialny organ. Należy opracować procedury ćwiczeń obejmujące element odzyskiwania systemu z nośnika kopii zapasowej.
- W przypadku systemów o dużym wpływie na działanie organizacji należy przeprowadzić pełne funkcjonalne ćwiczenie z częstotliwością określoną przez organizację. Pełne funkcjonalne ćwiczenie powinno obejmować przełączenie awaryjne systemu do zapasowej lokalizacji. Może to obejmować dodatkowe działania, takie jak pełne powiadomienie i zaangażowanie kluczowego personelu w lokalizacji odzyskiwania, odzyskiwanie serwerów lub bazy danych z nośnika kopii zapasowej lub konfiguracji serwera w zapasowej lokalizacji. Test powinien również obejmować pełne przywrócenie i odtworzenie systemu informatycznego do znanego stanu.

Tabela przedstawia przykładową aktywność TT&E z wykorzystaniem wytycznych NSC 800-53 i zgodnie z wymaganiami poziomu wpływu NSC 199.

**Tabela 3-6: Czynności ISCP TT&E**

| Zdarzenie TT&E | Przykłady aktywności | Wpływ na atrybut dostępności wg. NSC 199 |
|---|---|---|
| *ISCP Szkolenie (CP-3)* | Seminarium lub instruktaż używane do zapoznania personelu z ogólnym celem ISCP, fazami, działaniami oraz rolami i obowiązkami | Niski = Tak<br>Umiarkowany = Tak<br>Wysoki = Tak |
| Instruktaż *(CP-3)* | Instruktaż personelu awaryjnego na temat jego ról i obowiązków w ramach ISCP obejmujący szkolenie przypominające. W przypadku systemu o dużym wpływie należy uwzględnić zdarzenia symulowane. | Niski = Tak<br>Umiarkowany = Tak<br>Wysoki = Tak |
| *Testowanie / ćwiczenie planu awaryjnego (CP-4)* | Przetestuj i / lub przeprowadź plan awaryjny, aby określić skuteczność i gotowość organizacji. Może to obejmować zaplanowane i nieplanowane czynności utrzymaniowe. | Niski = Tak<br>Umiarkowany = Tak<br>Wysoki = Tak |

| Zdarzenie TT&E | Przykłady aktywności | Wpływ na atrybut dostępności wg. NSC 199 |
|---|---|---|
| *Ćwiczenia aplikacyjne (CP-4)* | Dyskusyjna symulacja sytuacji awaryjnej w nieformalnym, pozbawionym stresu środowisku; zaprojektowana w celu wywołania konstruktywnych dyskusji opartych na scenariuszach, w celu zbadania istniejącego ISCP i indywidualnego stanu gotowości. | Niski = Tak |
| *Ćwiczenia Funkcjonalne (CP-4)* | Symulacja zakłócenia za pomocą komponentu odzyskiwania systemu, takiego jak przywracanie kopii zapasowej na taśmie lub odzyskiwanie serwera. | Umiarkowany = Tak<br>Wysoki = Tak |
| *Pełnoskalowe ćwiczenia funkcjonalne (CP-4)* | Symulacja prowadząca do pełnego przywrócenia i odtworzenia systemu informatycznego do znanego stanu i zapewniająca zaznajomienie personelu z obiektem zapasowym. | Wysoki = Tak |

| Zdarzenie TT&E | Przykłady aktywności | Wpływ na atrybut dostępności wg. NSC 199 |
|---|---|---|
| *Odzyskiwanie systemu w zapasowym miejscu przetwarzania*<br>*(CP-4, CP-7)* | Testowanie planu awaryjnego w zapasowym miejscu przetwarzania, tak aby zapoznać personel awaryjny z obiektem i dostępnymi zasobami oraz ocenić możliwości lokalizacji zapasowej w zakresie wspierania operacji awaryjnych. Obejmuje pełne odzyskiwanie i powrót do normalnych operacji do znanego bezpiecznego stanu. W przypadku systemu o dużym wpływie, miejsce zapasowe powinno być w pełni skonfigurowane zgodnie ze zdefiniowanym planem. | Niski = opcjonalnie<br>Umiarkowany = opcjonalnie<br>Wysoki = Tak |
| *System kopii zapasowych*<br>*(CP-9)* | testowanie odzyskiwania informacji z kopii zapasowej w celu weryfikacji niezawodności nośnika i integralności informacji.<br>W przypadku systemu o dużym wpływie używaj kopii zapasowej z testową informacją i upewnij się, że kopie zapasowe są przechowywane w osobnym obiekcie). | Niski = opcjonalnie<br>Umiarkowany = Tak<br>Wysoki = Tak |

### 3.6 UTRZYMYWANIE PLANU

Plan, aby był skuteczny, musi być utrzymywany w stanie gotowości, który dokładnie odzwierciedla wymagania systemowe, procedury, strukturę organizacyjną i zasady. W trakcie SDLC systemy informacyjne podlegają częstym zmianom z powodu zmieniających się potrzeb biznesowych, aktualizacji technologii lub nowych polityk wewnętrznych lub zewnętrznych. Dlatego w ramach procesu zarządzania zmianami w organizacji konieczne jest regularne

sprawdzanie i aktualizowanie ISCP, aby zapewnić udokumentowanie nowych okoliczności i w razie potrzeby, zmianę środków awaryjnych. Jak określono w ramach kroku 6 RMF (ciągłe monitorowanie), ciągły proces monitorowania może zapewnić organizacjom skuteczne narzędzie do utrzymania planu, generowania bieżących aktualizacji planów bezpieczeństwa, raportów oceny bezpieczeństwa oraz planów działań i dokumentów etapowych w projektach.

Zasadniczo plan powinien być sprawdzany pod kątem dokładności i kompletności z częstotliwością określoną przez organizację lub za każdym razem, gdy wystąpią znaczące zmiany w dowolnym elemencie planu. Niektóre elementy, takie jak listy kontaktów, będą wymagały częstszych przeglądów i uaktualnień. Plany dotyczące systemów o umiarkowanym lub dużym wpływie powinny być częściej poddawane przeglądowi. Przeglądy planu powinny koncentrować się co najmniej na następujących elementach:

- Wymagania operacyjne;
- Wymagania bezpieczeństwa;
- Procedury techniczne;
- Sprzęt, oprogramowanie i inne wyposażenie (typy, specyfikacje i ilość);
- Nazwiska i dane kontaktowe członków zespołu;
- Nazwiska i dane kontaktowe dostawców, w tym PoC alternatywnych i zewnętrznych dostawców;
- Wymagania dotyczące alternatywnych i zewnętrznych obiektów;
- Istotne zapisy (elektroniczne i papierowe).

Ponieważ ISCP zawiera potencjalnie wrażliwe informacje operacyjne i osobowe, jego dystrybucja powinna być odpowiednio oznaczona i kontrolowana. Zazwyczaj w celu przechowywania kopie planu są przekazywane personelowi odpowiedzialnemu za odzyskiwanie. Kopia powinna być również przechowywana w alternatywnej lokalizacji i na nośniku kopii zapasowej. Przechowywanie kopii planu w alternatywnej lokalizacji zapewnia jej dostępność w przypadku, gdy z powodu awarii kopie planu nie będą dostępne

w lokalizacji dotkniętej awarią. Koordynator ISCP powinien prowadzić rejestr kopii planu i komu zostały one przekazane. Inne informacje, które powinny być przechowywane w planie, obejmują umowy z dostawcami (umowy SLA i inne umowy), licencje na oprogramowanie, instrukcje obsługi systemu, instrukcje bezpieczeństwa i procedury operacyjne.

Zmiany wprowadzone w planie, strategiach i politykach powinny być koordynowane za pośrednictwem Koordynatora ISCP, który w razie potrzeby powinien przekazywać zmiany przedstawicielom powiązanych planów lub programów. Koordynator ISCP powinien rejestrować modyfikacje planu przy użyciu rejestru zmian, który zawiera numer strony, komentarz do zmiany i datę zmiany. Zapis zmian, przedstawiony w tabeli, powinien zostać włączony do planu, jak omówiono w sekcji 4.1.

**Tabela 3-7: Przykład rejestru zmian**

| Rejestr Zmian | | | |
|---|---|---|---|
| **Nr strony** | **Komentarz zmiany** | **Data zmiany** | **Podpis** |
| | | | |
| | | | |

Koordynator ISCP powinien często kontaktować się ze współpracującymi wewnętrznymi komórkami organizacyjnymi i organizacjami zewnętrznymi oraz systemowymi PoC, aby zapewnić, że skutki spowodowane zmianami w dowolnej organizacji zostaną odzwierciedlone w planie awaryjnym. Należy zachować ścisłą kontrolę wersji, żądając zwrotu starych planów lub stron planu do koordynatora ISCP w zamian za nowy plan lub strony planu. Koordynator ISCP powinien również ocenić informacje uzupełniające, aby upewnić się, że informacje są aktualne i nadal odpowiednio spełniają wymagania systemowe. Informacje te obejmują:

- Umowę dotycząca zapasowej lokalizacji, w tym czasy testów;

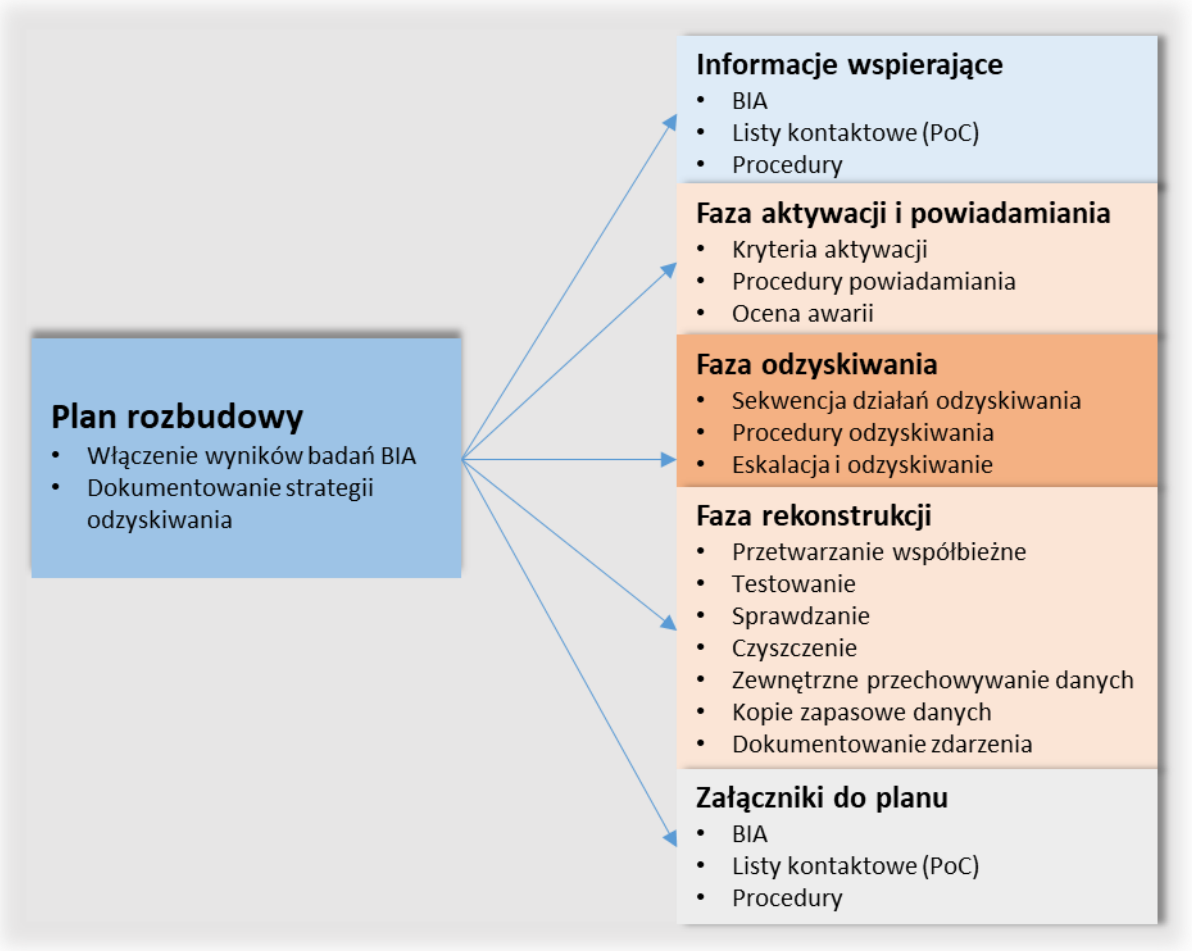
- Umowę dotyczącą przechowywania poza siedzibą kopii zapasowych;
- Licencje na oprogramowanie;
- MoU lub SLA dostawcy;
- Wymagania dotyczące sprzętu i oprogramowania;
- Umowy dotyczące połączeń międzysystemowych;
- Wymagania bezpieczeństwa;
- Strategię odzyskiwania;
- Polityki awaryjne;
- Materiały szkoleniowe i uświadamiające;
- Zakres testów;
- Inne plany, np. COOP, BCP.

Chociaż niektóre zmiany mogą być oczywiste, będą wymagały dodatkowej analizy. Kiedy nastąpi znacząca zmiana, BIA należy zaktualizować o nowe informacje, aby zidentyfikować nowe wymagania lub priorytety na wypadek awarii. W miarę pojawiania się nowych technologii, zabezpieczenia mogą być ulepszane, a strategie odzyskiwania mogą być modyfikowane. Utrzymywanie planu należy kontynuować również podczas przechodzenia systemu przez fazę wycofania podczas cyklu życia tak, aby zapewnić, że plan dokładnie odzwierciedla priorytety odzyskiwania i jednoczesne zmiany zachodzące w przetwarzaniu.

# ROZDZIAŁ 4 OPRACOWANIE PLANU AWARYJNEGO SYSTEMU INFORMATYCZNEGO

W tym rozdziale omówiono kluczowe elementy składające się na ISCP. Jak opisano w rozdziale 3, opracowanie ISCP jest krytycznym krokiem w procesie wdrażania kompleksowego programu planowania awaryjnego. Plan zawiera szczegółowe role, obowiązki, zespoły i procedury związane z przywracaniem systemu informatycznego po zakłóceniu. ISCP powinien udokumentować zdolności techniczne zaprojektowane do wspierania operacji awaryjnych i powinien być dostosowany do organizacji i jej wymagań. Plany muszą równoważyć szczegóły z elastycznością; zazwyczaj im bardziej szczegółowy plan, tym mniej skalowalne i wszechstronne podejście. Przedstawione informacje stanowią przewodnik, niemniej jednak format planu przedstawiony w tym dokumencie może zostać zmodyfikowany w razie potrzeby, aby lepiej spełniać określone wymagania systemowe, operacyjne i organizacyjne użytkownika. Dodatek A zawiera szablony, które organizacje mogą wykorzystać do opracowania ISCP dla swoich systemów informatycznych na odpowiednim poziomie wpływu NSC 199. Dostarczone informacje i szablony są przewodnikami i mogą być modyfikowane, dostosowywane tak, aby jak najlepiej spełniać określone wymagania systemowe, operacyjne i organizacyjne dotyczące planowania awaryjnego. Dodatek D omawia kwestie planowania dotyczące personelu, które powinny być skoordynowane z opracowaniem ISCP.

Jak pokazano na rysunku 4-1, plan awaryjny obejmuje pięć głównych elementów. Informacje dodatkowe i załączniki do planu zawierają szczegółowe informacje w celu utworzenia kompleksowego planu. Fazy Aktywacji i Powiadamiań, Odzyskiwanie oraz Odtwarzania, pokazują działania, które organizacja musi podjąć w przypadku awarii lub zagrożenia awarią. Każdy składnik planu omówiony zostanie w dalszych częściach tego rozdziału.




**Rysunek 4- 1 Struktura Planu Awaryjnego**

Plany należy sformatować tak, aby zapewnić szybkie i jasne wskazówki na wypadek, gdyby do wykonania operacji odzyskiwania został skierowany personel nieznający planu lub systemów. Plany powinny być jasne, zwięzłe i łatwe do wdrożenia w sytuacjach awaryjnych. Tam, gdzie to możliwe, należy stosować listy kontrolne i procedury krok po kroku. Zwięzły i dobrze sformatowany plan zmniejsza prawdopodobieństwo stworzenia zbyt złożonego lub niezrozumiałego planu.

## 4.1 INFORMACJE WSPIERAJĄCE PLAN AWARYJNY

Komponent informacji wspierających Plan awaryjny zawiera sekcję wstępu i koncepcji operacji, zapewniającą podstawowe informacje kontekstowe, które ułatwiają zrozumienie, wdrożenie i utrzymanie planu awaryjnego. Szczegóły tam zawarte pomagają zrozumieć

zastosowanie wskazówek, podejmować decyzje dotyczące korzystania z planu oraz zawierają informację o tym, gdzie można znaleźć powiązane plany i informacje wspomagające.

Sekcja wprowadzająca orientuje czytelnika co do rodzaju i lokalizacji informacji zawartych w planie. Zasadniczo sekcja zawiera tło, zakres i założenia, opisane poniżej.

- **Tło.** Ta podsekcja określa powód opracowania ISCP i określa cele planu;
- **Zakres.** Zakres określa poziom wpływu NSC 199 i powiązane RTO, a także alternatywne możliwości zapasowych lokalizacji i przechowywania danych (w stosownych przypadkach).
- **Założenia.** Ta sekcja zawiera listę założeń zastosowanych przy opracowywaniu ISCP, a także listę sytuacji, które nie mają zastosowania. Przykład założeń i sytuacji znajduje się w załączniku A - Przykładowe szablony planu awaryjnego systemu.

Sekcja poświęcona koncepcji operacji zawiera dodatkowe szczegóły na temat systemu informatycznego, trzech faz planu awaryjnego (Aktywacja i Powiadomienie, Odzyskiwanie, Odtwarzanie), a także opis ról i obowiązków związanych z planem awaryjnym systemu informatycznego. Sekcja ta może zawierać następujące elementy:

- **Opis systemu.** Konieczne jest zawarcie ogólnego opisu systemu informatycznego objętego planem awaryjnym. Opis powinien zawierać architekturę systemu informatycznego, lokalizację (lokalizacje) oraz wszelkie inne ważne aspekty techniczne. Przydatny jest schemat wejścia / wyjścia (I / O) i schemat architektury systemu, w tym urządzenia zabezpieczające (np. zapory sieciowe, połączenia wewnętrzne i zewnętrzne). Treść opisu systemu zwykle można pobrać z Planu bezpieczeństwa systemu.
- **Przegląd trzech faz.** Odzyskiwanie ISCP odbywa się w trzech fazach: (1) Aktywacja i Powiadamianie, (2) Odzyskiwanie i (3) Odtwarzanie.
- **Role i odpowiedzialność.** W sekcji role i odpowiedzialność przedstawiono ogólną strukturę zespołów awaryjnych, w tym mechanizmy i wymagania dotyczące hierarchii i koordynacji między zespołami. Sekcja zawiera także przegląd ról i obowiązków

członków zespołu w sytuacjach awaryjnych. Zespoły i członkowie zespołu powinni zostać wyznaczeni do określonych ról reagowania i odzyskiwania podczas aktywacji planu awaryjnego.

## 4.2 FAZA AKTYWACJI I POWIADAMIANIA

Faza Aktywacji i Powiadamiania określa wstępne działania podejmowane po wykryciu zakłócenia lub awarii systemu lub gdy wydaje się, że awaria jest nieuchronna. Faza ta obejmuje działania mające na celu powiadomienie personelu ds. odzyskiwania, przeprowadzenie oceny awarii i aktywację planu. Po zakończeniu fazy aktywacji i powiadamiania, pracownicy ISCP będą przygotowani do podjęcia działań naprawczych w celu przywrócenia funkcji systemu.

### 4.2.1 KRYTERIA AKTYWACJI I PROCEDURY

ISCP należy aktywować, jeśli jedno lub więcej kryteriów aktywacyjnych dla tego systemu jest spełnionych. Aktywacji planu dokonuje wyznaczony organ. Kryteria aktywacji w przypadku awarii lub zakłóceń systemu są unikatowe dla każdej organizacji i powinny zostać określone w polityce planowania awaryjnego. Kryteria mogą opierać się na:

- Stopniu uszkodzenia systemu (np. fizyczny, operacyjny lub kosztowy);
- Krytyczności systemu dla celu działania organizacji (np. zasób infrastruktury krytycznej);
- Przewidywanym czasie trwania awarii dłuższym niż RTO.

Gdy zostanie stwierdzone wyłączenie lub zakłócenie systemu, a koordynator ISCP ustali, że kryteria aktywacji zostały spełnione, powiadamiane są odpowiednie zespoły ds. odzyskiwania. Procedury powiadamiania powinny być zgodne z procedurami opisanymi w punkcie 4.2.2 poniżej.

### 4.2.2 PROCEDURY POWIADAMIANIA

Wystąpienie awarii lub zakłócenia może zostać wcześniej ogłoszone lub może nastąpić niespodziewanie. Na przykład często powiadamia się z wyprzedzeniem, że przewiduje się, iż warunki atmosferyczne wpłyną na dany obszar lub że w określonym dniu spodziewany jest

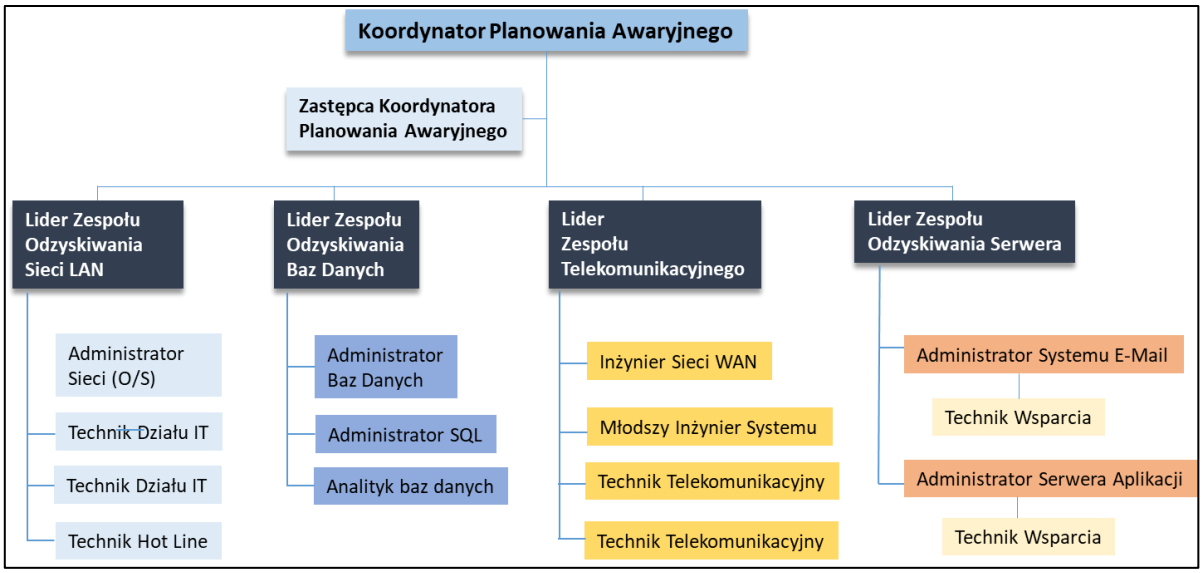
wirus komputerowy. Jednak awaria sprzętu może wystąpić niespodziewanie, samoistnie lub w wyniku działania przestępczego. Procedury powiadamiania powinny być udokumentowane w planie dla obu rodzajów sytuacji. Procedury powinny opisywać metody stosowane do powiadamiania personelu ds. odzyskiwania w godzinach pracy i poza godzinami pracy. Szybkie powiadamianie jest ważne dla ograniczenia skutków zakłóceń w systemie. W niektórych przypadkach może to zapewnić wystarczającą ilość czasu aby uniknąć poważnej awarii i personel systemu mógł bezpiecznie zamknąć system. Po wystąpieniu awarii lub zakłócenia należy wysłać powiadomienie do Zespołu ds. Oceny Awarii, aby mógł on ocenić status sytuacji i określić odpowiednie dalsze kroki. Procedury oceny awarii opisano w punkcie 4.2.3. Po zakończeniu oceny awarii należy powiadomić odpowiedni personel ds. odzyskiwania i wsparcia systemu.

Powiadomienia można realizować różnymi metodami, automatycznymi lub ręcznymi i obejmują one telefon stacjonarny, pocztę elektroniczną (e-mail), telefon komórkowy i komunikatory. Zautomatyzowane systemy powiadomień są zgodne z ustalonymi protokołami i kryteriami i mogą obejmować szybkie uwierzytelnianie i akceptację oraz bezpieczne przesyłanie wiadomości. Zautomatyzowane systemy powiadomień wymagają wstępnych inwestycji i uczenia się, ale dla niektórych organizacji mogą być skutecznym sposobem na zapewnienie szybkiego i skutecznego powiadomienia.

Powiadomienia wysyłane pocztą elektroniczną powinny być wykonywane ostrożnie, ponieważ nie ma sposobu, aby zapewnić odbiór i potwierdzenie. Chociaż poczta e-mail ma potencjał jako skuteczna metoda rozpowszechniania powiadomień na konta służbowe lub osobiste, nie ma jednak sposobu aby zagwarantować, że wiadomość zostanie przeczytana. W przypadku korzystania z metody powiadomień e-mail, personel odzyskiwania powinien zostać poinformowany o konieczności częstego i regularnego sprawdzania swoich kont. Powiadomienia wysyłane w godzinach pracy powinny być wysyłane na adres służbowy, natomiast osobiste wiadomości e-mail mogą być przydatne w przypadku awarii sieci lokalnej (LAN). Jeśli istnieje taka możliwość, informacje powiadamiające o nadejściu wiadomości powinny być wysyłane na urządzenie mobilne.

Strategia powiadamiania powinna określać procedury, których należy przestrzegać w przypadku braku kontaktu z konkretnym personelem. Procedury powiadamiania powinny być jasno udokumentowane w planie awaryjnym. Kopie procedur mogą być bezpiecznie przechowywane i aktywowane z różnych lokalizacjach. Popularną metodą ręcznego powiadamiania jest drzewo połączeń. Technika ta polega na przypisaniu obowiązków związanych z powiadomieniem konkretnym osobom, które z kolei są odpowiedzialne za powiadomienie innych pracowników ds. odzyskiwania. Drzewo połączeń powinno uwzględniać podstawowe i alternatywne metody kontaktu oraz powinno omawiać procedury, których należy przestrzegać, jeśli nie można się z kimś skontaktować.

Rysunek 4-2 przedstawia przykładowe drzewo połączeń.




**Rysunek 4- 2 Przykład drzewa połączeń**

Personel, który ma zostać powiadomiony, powinien być wyraźnie określony na listach kontaktów dołączonych do planu. Lista powinna identyfikować personel według roli w zespole, nazwiska i danych kontaktowych (np. miejsca pracy, telefonu komórkowego, adresów e-mail i adresów domowych).

Wpis może posiadać następujący format:

Zespół oprogramowania systemowego
Lider Zespołu—Funkcja podstawowa
Jan Kowalski
Ulica Klonowa 123
Kod Pocztowy, Miasto
Dom: 123 456 7890
Praca: 123 567 8901
Kom.: 123 678 9012
e-mail: jkowalski@organizacja.ext ; jk@domowy.ext

Powiadomienia należy również wysyłać do PoC organizacji zewnętrznych, na które mogą mieć wpływ negatywne skutki zakłócenia, o ile nie będą świadome zaistniałej sytuacji. W zależności od rodzaju awarii lub zakłóceń, PoC może mieć udział w obowiązkach związanych z odzyskiwaniem. Dla każdej organizacji zewnętrznej, która ma związek z systemem należy zidentyfikować PoC. Punkty kontaktowe powinny być wymienione w załączniku do planu.

Rodzaj informacji przekazywanych powiadamianym osobom powinien być udokumentowany w planie. Ilość i szczegółowość przekazywanych informacji może zależeć od powiadomienia konkretnego zespołu. W razie potrzeby informacje o powiadomieniu mogą obejmować:

- Charakter awarii lub zakłóceń, które miały miejsce lub mogą się wydarzyć;
- Wszelkie znane szacunki dotyczące awarii;
- Szczegóły odpowiedzi na zakłócenie i odzyskiwania;
- Gdzie i kiedy zwołać spotkanie w celu uzyskania instrukcji lub dalszych działań dotyczących odpowiedzi;
- Instrukcje przygotowania do relokacji do zapasowego miejsca pracy (jeśli dotyczy);
- Instrukcje wykonywania powiadomień za pomocą drzewa połączeń (jeśli dotyczy).

### 4.2.3 OCENA AWARII

Celem ustalenia, w jaki sposób ISCP zostanie wdrożony po zakłóceniu lub awarii systemu, konieczna jest ocena charakteru i zakresu zakłócenia. Ocenę awarii należy zakończyć tak szybko, jak tylko pozwalają na to warunki, przy czym bezpieczeństwo personelu pozostaje najwyższym priorytetem. Jeśli to możliwe, Zespół ds. Oceny Awarii powinien być pierwszym zespołem powiadomionym o zakłóceniu. Procedury oceny awarii mogą być unikatowe dla konkretnego systemu, ale należy uwzględnić następujące minimalne obszary:

- Przyczyna awarii lub zakłóceń;
- Możliwość dodatkowych zakłóceń lub szkód;
- Status infrastruktury fizycznej (np. integralność strukturalna sali komputerowej, stan energii elektrycznej, telekomunikacji, ogrzewania, wentylacji i klimatyzacji [HVAC]);
- Stan inwentaryzacyjny i funkcjonalny wyposażenia systemu (np. w pełni funkcjonalny, częściowo funkcjonalny, niefunkcjonalny);
- Przyczyna uszkodzenia sprzętu lub danych systemu (np. woda, ogień i ciepło, uderzenie fizyczne, przepięcie energetyczne);
- Elementy do wymiany (np. sprzęt, oprogramowanie, oprogramowanie układowe, materiały pomocnicze);
- Szacowany czas na przywrócenie normalnych usług.

Personel odpowiedzialny za ocenę awarii powinien być w stanie wykonać procedury również w sytuacji, gdyby plan był niedostępny w danej sytuacji. Po ustaleniu wpływu na system, odpowiednie zespoły powinny zostać powiadomione o zaistniałej sytuacji i planowanej reakcji na nią. W oparciu o wyniki oceny awarii powiadomienia ISCP mogą być podejmowane dalsze działania przy użyciu procedur opisanych w punkcie 4.2.2.

## 4.3 FAZA ODZYSKIWANIA

Formalne operacje odzyskiwania zaczynają się po aktywacji ISCP, zakończeniu oceny awarii (jeśli to możliwe), powiadomieniu personelu i zmobilizowaniu odpowiednich zespołów.

Działania w fazie odzyskiwania koncentrują się na wdrażaniu strategii odzyskiwania w celu przywrócenia możliwości działania systemu, naprawy uszkodzeń i wznowienia możliwości operacyjnych w stałej lub zapasowej lokalizacji. Po zakończeniu fazy odzyskiwania, system informatyczny będzie funkcjonalny i będzie mógł wykonywać funkcje określone w planie. W zależności od strategii odzyskiwania określonych w planie, funkcje te mogą obejmować tymczasowe ręczne przetwarzanie, odzyskiwanie i działanie w alternatywnym systemie lub przenoszenie i odzyskiwanie w zapasowym miejscu pracy. Możliwe jest, że na tym etapie zostaną odzyskane tylko zasoby systemowe uznane za priorytetowe w BIA.

### 4.3.1 SEKWENCJA DZIAŁAŃ ODZYSKIWANIA

Podczas odzyskiwania złożonego systemu, takiego jak sieć rozległa (WAN) lub wirtualna sieć lokalna (VLAN) obejmująca wiele niezależnych komponentów, procedury odzyskiwania powinny odzwierciedlać priorytety systemu określone w BIA. Sekwencja działań powinna odzwierciedlać MTD systemu, aby uniknąć znaczącego wpływu na systemy powiązane. Procedury powinny być zapisywane w stopniowym, sekwencyjnym formacie, aby komponenty systemu mogły zostać przywrócone w logiczny sposób. Na przykład, jeśli po zakłóceniu jest odzyskiwana sieć LAN, najbardziej krytyczne serwery należy odzyskać przed innymi, mniej krytycznymi urządzeniami, takimi jak drukarki. Podobnie, aby odzyskać serwer aplikacji, procedury powinny najpierw dotyczyć przywracania i weryfikacji systemu operacyjnego, zanim aplikacja i jej dane zostaną odzyskane. Procedury powinny również obejmować kroki eskalacji i instrukcje dotyczące koordynacji z innymi zespołami, w stosownych przypadkach, w przypadku wystąpienia określonych sytuacji, takich jak:

- Działanie nie zostało zakończone w oczekiwanym czasie;
- Kluczowy krok został zakończony;
- Muszą być zamawiane nowe komponenty systemu;
- Istnieją inne problemy specyficzne dla systemu.

Jeśli warunki wymagają odzyskania systemu w zapasowym miejscu pracy, będą musiały być tam przekazane lub pozyskane niektóre materiały lub komponenty systemu. Może to

obejmować wysyłkę nośników kopii zapasowych danych z zewnętrznego magazynu, sprzętu, kopii planu odzyskiwania i programów. Procedury powinny wyznaczyć odpowiedni zespół lub członków zespołu do koordynowania wysyłki sprzętu, danych i istotnych zapisów. W razie potrzeby, w planie należy umieścić odniesienia do odpowiednich dodatków, takich jak listy urządzeń lub dane kontaktowe dostawcy. Procedury powinny jasno opisywać wymagania dotyczące pakowania, transportu i zakupu materiałów wymaganych do odzyskania systemu.

### 4.3.2 PROCEDURY ODZYSKIWANIA

Aby ułatwić operacje w fazie odzyskiwania, ISCP powinien zapewnić szczegółowe procedury odzyskiwania systemu lub komponentów informatycznych do ustalonego stanu. Biorąc pod uwagę dużą różnorodność typów systemów, konfiguracji i aplikacji, prezentowany przewodnik planowania nie zawiera szczegółowych procedur odzyskiwania. Zagadnienia dotyczące odzyskiwania są szczegółowo opisane dla każdego rodzaju platformy w Rozdziale 5.

Procedury należy przypisać do odpowiedniego Zespołu ds. odzyskiwania i zazwyczaj dotyczą one następujących działań:

- Uzyskanie zezwolenia na dostęp do uszkodzonych obiektów;
- Powiadamianie wewnętrznych i zewnętrznych partnerów biznesowych związanych z systemem;
- Pozyskanie niezbędnych materiałów biurowych i miejsca do pracy;
- Uzyskiwanie i instalowanie niezbędnych komponentów sprzętowych;
- Uzyskiwanie i ładowanie nośników kopii zapasowych;
- Przywracanie krytycznego systemu operacyjnego i oprogramowania aplikacyjnego;
- Przywracanie danych systemowych do ustalonego stanu;
- Testowanie funkcjonalności systemu, w tym zabezpieczeń;
- Łączenie systemu z siecią lub innymi systemami zewnętrznymi;
- Sprawdzenie skuteczności działania sprzętu alternatywnego.

Procedury odzyskiwania powinny być napisane prostym, komunikatywnym językiem, krok po kroku. Aby zapobiec trudnościom lub nieporozumieniom w sytuacjach awaryjnych, nie należy zakładać ani pomijać żadnych kroków proceduralnych. Jeśli systemu nie można prawidłowo odzyskać, przydatny do dokumentowania przebiegu procedur odzyskiwania sekwencyjnego i rozwiązywania problemów jest format listy kontrolnej.

Rysunek 4-3 przedstawia częściowy przykład proceduralnej listy kontrolnej dla zespołu przywracania sieci LAN.

**Przykładowy Proces Odzyskiwania dla Zespołu Odzyskiwania LAN:**

Do odzyskiwania pliku z kopii zapasowych używane są następujące procedury.

Zespół odzyskiwania sieci LAN jest odpowiedzialny za ponowne załadowanie wszystkich krytycznych plików niezbędnych do kontynuowania działalności.

1. Zidentyfikuj plik i jego datę, który ma zostać odzyskany.
2. Zidentyfikuj numer nośnika za pomocą dziennika nośników.
3. Jeśli nośnika nie ma na miejscu, poproś o nośnik z obiektu, w którym jest składowany; wypełnij i podpisz zamówienie.
4. Po odebraniu nośnika zapisz datę i godzinę.
5. Włóż nośnik do napędu i rozpocznij proces odzyskiwania.
6. Gdy plik zostanie odzyskany, powiadom Lidera Zespołu Odzyskiwania sieci LAN.

**Rysunek 4-3 Przykład procesu odzyskiwania**

### 4.3.3 ESKALACJA ODZYSKIWANIA I POWIADOMIENIA

Jak określono w BIA, komponenty systemu, infrastruktura i powiązane urządzenia są kluczowymi elementami wspierającymi codzienne procesy biznesowe. Systemy, aplikacje i infrastruktura, które wykorzystują użytkownicy tych procesów, podlegają zdarzeniom powodującym przerwy w świadczeniu usług. Włączenie komponentu eskalacji

i powiadomienia w fazie odzyskiwania, pomaga zapewnić przestrzeganie ogólnego, powtarzalnego, ustrukturyzowanego, spójnego i mierzalnego procesu odzyskiwania.

Skuteczne procedury eskalacji i powiadamiania powinny określać i opisywać zdarzenia, progi lub inne rodzaje zdarzeń inicjujących, które są niezbędne do dodatkowych działań. Działania takie obejmowałyby dodatkowe powiadomienia dla większej liczby pracowników ds. odzyskiwania, przekazywane do kierownictwa wiadomości i aktualizacje statusu oraz powiadomienia o niezbędnych dodatkowych zasobach. Dla zespołów lub osób należy wprowadzić procedury w celu ustalenia jasnego zestawu wydarzeń, działań i wyników, a także odpowiednio je udokumentować.

## 4.4 FAZA ODTWARZANIA

Faza odtwarzania jest trzecią i ostatnią fazą wdrożenia ISCP. Określa działania podejmowane w celu przetestowania i potwierdzenia zdolności i funkcjonalności systemu. Podczas odtwarzania, czynności odzyskiwania są już zakończone i wznawiane są normalne operacje systemowe. Jeśli pierwotnego obiektu nie można odzyskać, działania na tym etapie można również zastosować do przygotowania nowej stałej lokalizacji spełniającej wymagania systemu. Ta faza składa się z dwóch głównych działań: sprawdzania poprawności odzyskiwania i dezaktywacji planu.

Sprawdzanie poprawności odzyskiwania zwykle obejmuje następujące kroki:

- **Przetwarzanie Współbieżne**. Przetwarzanie współbieżne to proces uruchamiania systemu w dwóch oddzielnych lokalizacjach jednocześnie, do czasu uzyskania określonego poziomu pewności, że odzyskany system działa poprawnie i bezpiecznie.
- **Testowanie danych walidacyjnych**. Testowanie danych to proces testowania i sprawdzania poprawności odzyskanych danych w celu upewnienia się, że pliki danych lub bazy danych zostały całkowicie odzyskane i są aktualne według stanu zapisanego na ostatniej dostępnej kopii zapasowej.

- **Sprawdzanie poprawności działania**. Testowanie funkcjonalności to proces sprawdzania, czy cała funkcjonalność systemu została przetestowana i czy system jest gotowy do powrotu do normalnej pracy.

Po pomyślnym zakończeniu testów walidacyjnych, personel ISCP będzie przygotowany do zadeklarowania, że wysiłki związane z odtworzeniem zostały zakończone i system działa normalnie. Deklaracja ta może zostać złożona w dzienniku odzyskiwania / odtwarzania lub w innej dokumentacji opisującej czynności związane z odtwarzaniem. Koordynator ISCP, w porozumieniu z właścicielem systemu informatycznego, ISSO, SAISO oraz w porozumieniu z organem zatwierdzającym, musi ustalić, czy system przeszedł znaczącą zmianę i będzie wymagał ponownej oceny i ponownej autoryzacji. Wykorzystanie strategii / programu ciągłego monitorowania może kierować zakresem ponownej autoryzacji, aby skupić się na tych zabezpieczeniach środowiska / obiektu i wszelkich innych zabezpieczeniach, na które miałyby wpływ wysiłki związane z odtworzeniem.

Dezaktywacja planu to proces przywracania systemu do normalnego działania i finalizowania działań związanych z odtwarzaniem w celu przygotowania systemu na wypadek kolejnej awarii lub zakłócenia. Działania te obejmują:

- **Powiadomienia**. O powrocie do normalnych operacji użytkownicy powinni zostać powiadomieni przez koordynatora ISCP (lub wyznaczoną osobę) przy użyciu wstępnie zdefiniowanych procedur powiadamiania.
- **Oczyszczanie**. Oczyszczanie to proces czyszczenia miejsca pracy lub demontażu tymczasowych lokalizacji odzyskiwania, uzupełniania zapasów, zwracania instrukcji lub innej dokumentacji do ich pierwotnych lokalizacji oraz przygotowania systemu do kolejnego zdarzenia awaryjnego.
- **Zewnętrzne przechowywanie danych**. Jeśli używane jest zewnętrzne przechowywanie danych, należy udokumentować procedury zwrotu odzyskanego nośnika kopii zapasowej lub nośnika instalacyjnego do jego zewnętrznego miejsca przechowywania.

- **Kopie zapasowe danych**. Tak szybko, jak to uzasadnione po odtworzeniu, należy w pełni wykonać kopię zapasową systemu i zapisać nową kopię obecnego systemu operacyjnego na potrzeby przyszłych prób przywrócenia systemu. Pełna kopia zapasowa powinna być przechowywana z innymi kopiami zapasowymi systemu i powinna być zgodna z odpowiednimi zabezpieczeniami.
- **Dokumentacja zdarzenia**. Wszystkie zdarzenia związane z odzyskiwaniem i odtwarzaniem powinny być dobrze udokumentowane, w tym podjęte działania i problemy napotkane podczas wysiłków związanych z odzyskiwaniem i odtwarzaniem. Raport z działań po zakończeniu wraz z wyciągniętymi wnioskami powinien zostać udokumentowany i dołączony do aktualizacji ISCP.

Po zakończeniu wszystkich działań i kroków oraz aktualizacji dokumentacji, ISCP można formalnie dezaktywować. Ogłoszenie z deklaracją zakończenia działań należy wysłać do wszystkich kontaktów biznesowych i technicznych.

## 4.5 ZAŁĄCZNIKI DO PLANU

Załączniki do planu awaryjnego zawierają kluczowe szczegóły nie zawarte w głównej części planu. Ogólnie ujmując, załączniki do planu awaryjnego obejmują:

- Informacje kontaktowe dla personelu zespołu planowania awaryjnego;
- Informacje kontaktowe dostawcy, w tym magazynowanie poza siedzibą i zapasowe miejsca pracy PoC;
- BIA;
- Szczegółowe procedury odzyskiwania i listy kontrolne;
- Szczegółowe procedury testowania walidacji i listy kontrolne;
- Listy wymagań sprzętowych i systemowych sprzętu, oprogramowania, oprogramowania układowego i innych zasobów wymaganych do obsługi operacji systemowych. Dla każdego wpisu należy podać szczegółowe informacje, w tym numer modelu lub wersji, specyfikacje i ilość;

- Alternatywne procedury przetwarzania dla procesów biznesowych, które mogą wystąpić podczas przywracania systemu;
- Procedury testowania i konserwacji ISCP;
- Połączenia międzysystemowe (systemy, które bezpośrednio się łączą lub wymieniają informacje);
- Umowy SLA dostawców, wzajemne umowy z innymi organizacjami oraz inne ważne dokumenty.

# ROZDZIAŁ 5 UWAGI TECHNICZNE DOTYCZĄCE PLANOWANIA AWARYJNEGO

Niniejszy rozdział uzupełnia wytyczne dotyczące procesu i ram przedstawionych we wcześniejszych rozdziałach, omawiając kwestie techniczne dotyczące planowania awaryjnego dla określonych rodzajów systemów informatycznych. Informacje przedstawione w tej sekcji pomogą czytelnikowi w wyborze, opracowaniu i wdrożeniu określonych technicznych strategii awaryjnych w zależności od rodzaju systemu informatycznego. Ponieważ każdy system jest unikatowy, rozważania zostały przedstawione na poziomie, z którego może skorzystać najszersza grupa odbiorców. Lista platform nie jest wyczerpująca, ale jest reprezentatywna dla często spotykanych systemów w produkcji lub we wdrożeniu. Nie wszystkie przedstawione informacje mogą dotyczyć konkretnego systemu informatycznego. Koordynator ISCP powinien odpowiednio wziąć pod uwagę te okoliczności i dostosować je do konkretnych wymagań awaryjnych systemu. W tej sekcji omówiono następujące reprezentatywne typy platform:

- Systemy klient / serwer;
- Systemy telekomunikacyjne;
- Systemy klasy mainframe.

Dla każdego typu systemu, środki awaryjne są rozpatrywane z dwóch perspektyw. Po pierwsze, dokument omawia wymagania techniczne lub czynniki, które koordynator ISCP powinien wziąć pod uwagę przy planowaniu strategii odzyskiwania systemu podczas cyklu życia systemu SDLC. Po drugie, dokument zawiera rozwiązania oparte na technologii dla każdego rodzaju systemu.

## 5.1 CZYNNIKI WSPÓLNE

Zagadnienia techniczne i rozwiązania omówione w tej sekcji obejmują środki zapobiegawcze omówione w sekcji 3.3 oraz środki odzyskiwania opisane w sekcji 3.4. Przy opracowywaniu rozwiązań technicznych planów awaryjnych należy wziąć pod uwagę kilka obszarów, niezależnie od platformy lub rodzaju systemu. Niniejsze rozważania stanowią wspólną podstawę dla wszelkiego rodzaju działań związanych z planowaniem awaryjnym. Kilka z tych

środków awaryjnych jest wspólnych dla wszystkich systemów informatycznych. Typowe zagadnienia obejmują:

- Wykorzystanie informacji zebranych w procesie BIA;
- Opracowywanie zasad i procedur bezpieczeństwa, integralności i tworzenia kopii zapasowych danych;
- Ochrona sprzętu i zasobów systemowych;
- Przestrzeganie i zgodność z zabezpieczeniami określonymi w NSC 800-53;
- Opracowanie pierwotnych i zapasowych miejsc pracy z odpowiednio dobranymi i skonfigurowanymi systemami zarządzania energią i kontrolą środowiska;

Wykorzystanie procesów wysokiej dostępności (*ang. high availability - HA*) w celu zapewnienia elastycznego dostępu online w czasie rzeczywistym do alternatywnych zasobów systemowych. HA oznacza systemy, które mogą osiągnąć czas sprawności wynoszący 99,999% lub więcej. Należy pamiętać, że HA jest procesem osiągania wysokiej dostępności i nie należy go mylić z systemami kategorii o wysokim wpływie opisanym w NSC 199.

### 5.1.1 WYKORZYSTANIE BIA

BIA jest pierwotnym źródłem do określania strategii planowania odporności i planowania awaryjnego. Wyniki BIA określają, jak krytyczny jest system dla obsługiwanych procesów biznesowych, jaki wpływ może mieć utrata systemu na organizację i RTO systemu. Wyniki BIA mogą pomóc określić rodzaj i częstotliwość tworzenia kopii zapasowych, potrzebę redundancji lub dublowania danych oraz rodzaj zapasowych miejsc pracy niezbędnych do osiągnięcia celów odzyskiwania systemu. Każda z tych decyzji strategicznych, w zależności od dostępności, ma wpływ na koszt lub odzyskiwanie. Wpływ na dostępność i odzyskiwanie omówiono w dalszej części tego rozdziału.

### 5.1.2 UTRZYMANIE BEZPIECZEŃSTWA, INTEGRALNOŚCI KOPII ZAPASOWYCH DANYCH

Utrzymanie integralności i bezpieczeństwa danych systemowych i oprogramowania jest kluczowym elementem planowania awaryjnego. Integralność danych polega na zapewnieniu bezpieczeństwa i dokładności danych na podstawowych urządzeniach pamięci masowej. Dostępnych jest kilka metod utrzymania integralności przechowywanych danych. Metody te wykorzystują procesy nadmiarowości i odporności na uszkodzenia do przechowywania danych na więcej niż jednym dysku i eliminują utratę danych w wyniku awarii jednego dysku. Bezpieczeństwo danych obejmuje ochronę danych, zarówno w siedzibach organizacji, jak i poza nimi, przed nieautoryzowanym dostępem lub wykorzystaniem. Szyfrowanie jest powszechną metodą zabezpieczania przechowywanych danych systemowych. Szyfrowanie jest najskuteczniejsze, gdy stosuje się je zarówno do podstawowego urządzenia do przechowywania danych, jak i na nośniku kopii zapasowej przekazywanym do lokalizacji poza siedzibą. W przypadku korzystania z szyfrowania do przechowywania danych poza siedzibą ważne jest, aby czytniki nośników (np. napędy taśm, czytniki CD lub DVD) dostępne w zapasowym miejscu pracy były zdolne poprawnie odczytać zaszyfrowane dane podczas procesu odzyskiwania. Należy ustanowić proces zarządzania kluczami, tak aby zaszyfrowane dane były zawsze dostępne. Istotne materiały, którymi są dane używane do ustanowienia i utrzymania kluczy, muszą być w organizacji prawidłowo zarządzane. Klucze powinny być przechowywane oddzielnie od zaszyfrowanych nimi danych kopii zapasowych, ale dostępne w przypadku konieczności ich odszyfrowania.

Przechowywanie kopii zapasowych danych w bezpiecznej lokalizacji poza siedzibą pozwala na łatwy dostęp do kopii zapasowych podczas zdarzenia awaryjnego. Skuteczny proces tworzenia kopii zapasowych danych ma kluczowe znaczenie dla ogólnej strategii odzyskiwania. Kopie zapasowe danych są tworzone głównie w celu odzyskiwania tych danych. Kopie zapasowe można wykonywać wieloma różnymi metodami i technikami. Określenia MTD i wymagania bezpieczeństwa z BIA pomagają określić najlepszą metodę tworzenia kopii zapasowych niezbędnych do odzyskiwania określonego systemu.

Kopie zapasowe danych należy regularnie wykonywać we wszystkich systemach. Kopie zapasowe systemów można tworzyć dla pojedynczych komputerów lub na scentralizowanym

urządzeniu magazynującym, takim jak pamięć sieciowa (*ang. network attached storage - NAS*) lub sieć pamięci masowej (*ang. storage area network - SAN*). Istnieją trzy popularne metody wykonywania kopii zapasowych systemu:

- **Pełna.** Pełna kopia zapasowa przechwytuje wszystkie pliki na dysku lub w folderze wybranym do utworzenia kopii zapasowej. Ponieważ wszystkie pliki z kopii zapasowej są zapisywane na jednym nośniku lub zestawie nośników, zlokalizowanie określonego pliku lub grupy plików jest proste. Jednak czas wymagany do wykonania pełnej kopii zapasowej może być długi. Ponadto utrzymanie wielu iteracji pełnych kopii zapasowych plików, które nie zmieniają się często (takich jak pliki systemowe), może prowadzić do nadmiernych, niepotrzebnych wymagań dotyczących przechowywania tych kopii.
- **Przyrostowa**. Przyrostowa kopia zapasowa przechwytuje pliki, które zostały utworzone lub zmienione w odniesieniu do ostatniej kopii zapasowej, niezależnie od typu kopii zapasowej. Przyrostowe kopie zapasowe zapewniają bardziej wydajne wykorzystanie nośników pamięci, a czasy tworzenia kopii zapasowych są krótsze. Jednak w celu odzyskania systemu z przyrostowej kopii zapasowej mogą być wymagane nośniki z różnych operacji tworzenia kopii zapasowych. Rozważmy na przykład przypadek, w którym należy odzyskać katalog. Jeśli ostatnia pełna kopia zapasowa została wykonana trzy dni wcześniej, a jeden plik zmieniał się każdego dnia, wówczas do przywrócenia całego katalogu byłby potrzebny nośnik dla pełnej kopii zapasowej i przyrostowe kopie zapasowe każdego dnia.
- **Różnicowa**. Różnicowa kopia zapasowa przechowuje pliki, które zostały utworzone lub zmodyfikowane od czasu utworzenia ostatniej pełnej kopii zapasowej. Dlatego jeśli plik zostanie zmieniony po poprzedniej pełnej kopii zapasowej, różnicowa kopia zapasowa będzie zapisywać plik za każdym razem, aż do wytworzenia następnej pełnej kopii zapasowej. Różnicowa kopia zapasowa zajmuje mniej czasu niż pełna kopia zapasowa. Przywracanie z różnicowej kopii zapasowej może wymagać mniejszej liczby nośników niż przyrostowej kopii zapasowej, ponieważ potrzebny byłby tylko pełny nośnik kopii zapasowej i ostatni nośnik różnicowy. Wadą jest to, że różnicowe

tworzenie kopii zapasowych trwa dłużej niż przyrostowe, ponieważ ilość danych od ostatniej pełnej kopii zapasowej, aż do wykonania następnej pełnej kopii zapasowej, rośnie każdego dnia.

Można stosować kombinację operacji tworzenia kopii zapasowych w zależności od konfiguracji systemu i wymagań dotyczących odzyskiwania. Na przykład pełna kopia zapasowa może zostać wykonana w weekend, a kopie różnicowe wykonywane każdego wieczoru. Opracowując zasady tworzenia kopii zapasowych systemu, należy wziąć pod uwagę następujące pytania:

- Gdzie i jak będą przechowywane nośniki?
- Jakie dane powinny być archiwizowane i jak często powinny być archiwizowane?
- Jak szybko należy odzyskać kopie zapasowe w razie niebezpieczeństwa?
- Kto jest upoważniony do pobierania nośników?
- Gdzie zostanie dostarczony nośnik i jaki jest harmonogram rotacji nośników kopii zapasowych?
- Kto przywróci dane z nośnika?
- Jak wygląda sposób oznakowania nośników?
- Jak długo będzie przechowywany nośnik kopii zapasowej?
- Kiedy nośniki są przechowywane na miejscu, jakie zabezpieczenia środowiskowe są zapewniane w celu przechowania nośników?
- Jaki nośnik kopii zapasowej jest odpowiedni dla danych typów kopii zapasowych, które należy wykonać?

Wybierając odpowiednie rozwiązanie do tworzenia kopii zapasowych, należy wziąć pod uwagę pewne czynniki:

- **Interoperacyjność urządzeń**. Aby ułatwić odzyskiwanie, urządzenie do tworzenia kopii zapasowych musi być zgodne z systemem operacyjnym platformy i aplikacjami

oraz powinno być łatwe do zainstalowania na różnych modelach lub typach systemów.

- **Wolumin magazynu**. Pojemność pamięci masowej przeznaczonej do wykonywania kopii zapasowych jest określana przez ilość danych, które należy przechować.
- **Czas życia nośnika**. Każdy rodzaj nośnika ma inne przeznaczenie i czas przechowywania, po przekroczeniu którego nośnik traci swoje właściwości i nie można na nim polegać w procesie skutecznego odzyskiwania danych.
- **Oprogramowanie do tworzenia kopii zapasowych**. Wybierając odpowiednie rozwiązanie do tworzenia kopii zapasowych, należy wziąć pod uwagę oprogramowanie lub metodę wykonania kopii zapasowej danych. W niektórych przypadkach rozwiązanie do tworzenia kopii zapasowych może być tak proste, jak kopiowanie plików za pomocą menedżera plików systemu operacyjnego.
  W przypadkach większych transferów danych, może być potrzebna aplikacja innej firmy do zautomatyzowania i zaplanowania tworzenia kopii zapasowej danych.

### 5.1.3 OCHRONA ZASOBÓW

Jednym z celów polityki planowania awaryjnego jest uodpornienie systemu na awarie środowiskowe i awarie na poziomie komponentów, które w przeciwnym razie spowodowałyby awarie całego systemu. Istnieje kilka metod zwiększania odporności wartościowego sprzętu i oprogramowania. Określenie odpowiednich metod powinno opierać się na decyzjach podejmowanych z uwzględnieniem ryzyka. W zależności od wyników procesu zarządzania ryzykiem, metody te mogą, ale nie muszą mieć zastosowania do konkretnego systemu.

System i jego dane mogą ulec uszkodzeniu w wyniku awarii zasilania. Aby zapobiec takiemu uszkodzeniu, krytyczny sprzęt, taki jak serwery, można wyposażyć w podwójne zasilacze. Oba zasilacze powinny być używane jednocześnie (w tym jeden w stanie operacyjnym, a drugi w stanie gorącej rezerwy), tak aby w przypadku przegrzania lub bezużyteczności głównego zasilacza druga jednostka stała się głównym źródłem zasilania, co nie spowodowałoby zakłóceń w systemie. Drugi zasilacz chroni przed awarią sprzętu, ale nie

przed awarią zasilania. W przypadku utraty zasilania, system może być chroniony zasilaczem bezprzerwowym (UPS). UPS zwykle zapewnia 30 do 60 minut tymczasowego zasilania awaryjnego, aby umożliwić płynne wyłączenie systemu. UPS może również chronić przed wahaniami napięcia zasilania, filtrując przychodzące zasilanie i zapewniając gwarantowane parametry źródła zasilania. W dużych systemach nawet 60 minutowe zasilacze nie gwarantują czasu niezbędnego do kontrolowanego zamknięcia systemu, a zwiększanie czasu pracy z akumulatorów jest ekonomicznie nieopłacalne. W takim przypadku, a także jeśli wymagana jest wysoka dostępność, może być potrzebny agregat prądotwórczy. Można go podłączyć bezpośrednio do systemu zasilania urządzeń i skonfigurować tak, aby uruchamiał się automatycznie po wykryciu przerwy w zasilaniu. Połączenie systemu UPS / agregat może zapewnić filtrowane, bezpieczne zasilanie systemu, o ile agregat ma zapewnione paliwo. Dostępność paliwa należy wziąć pod uwagę wybierając zasilacz UPS / agregat do obsługi środowiska systemowego.

Oprócz tworzenia kopii zapasowych danych, organizacje powinny również wykonać kopię zapasową oprogramowania systemowego i sterowników. Organizacje powinny przechowywać oprogramowanie i licencje na oprogramowanie w innej lokalizacji. Obejmuje to oryginalny nośnik instalacyjny, warunki licencji i klucze licencyjne, jeśli są wymagane. Kopie zapasowe obrazów dla systemów klienckich (takich jak komputery stacjonarne i przenośne) powinny być również archiwizowane i przechowywane w innej lokalizacji, wraz z pełną dokumentacją oprogramowania zawartego w ładowanym obrazie, wszelkie informacje konfiguracyjne dla konkretnego typu komputera, dla którego obraz jest przeznaczony i instrukcje instalacji.

Organizacje mogą wykorzystywać zewnętrznych dostawców do odzyskiwania danych z uszkodzonych urządzeń pamięci masowej. Organizacje powinny rozważyć ryzyko związane z bezpieczeństwem obsługi danych przez firmę zewnętrzną i dopilnować, aby przed oddaniem sprzętu przeprowadzono odpowiednią weryfikację bezpieczeństwa dostawcy usług. Usługodawca i pracownicy powinni podpisać umowy o zachowaniu poufności, oraz być odpowiednio związani przestrzeganiem zasad bezpieczeństwa obowiązujących w danej organizacji.

### 5.1.4 PRZESTRZEGANIE ZABEZPIECZEŃ

Zabezpieczenia ustanowione w NSC 800-53 zapewniają wymagane podstawy do ustanowienia zasad bezpieczeństwa, integralności i bezawaryjności systemu informatycznego. Przestrzeganie tych zabezpieczeń w procesie planowania awaryjnego pomaga chronić system informatyczny przed zagrożeniami, które mogą zakłócać operacje biznesowe organizacji.

### 5.1.5 IDENTYFIKACJA ALTERNATYWNYCH LOKALIZACJI DO PRZECHOWYWANIA I PRZETWARZANIA DANYCH

Nośniki kopii zapasowych powinny być przechowywane poza siedzibą firmy w bezpiecznym, kontrolowanym środowiskowo miejscu. Wybierając lokalizację poza siedzibą, należy wziąć pod uwagę godziny pracy lokalizacji, łatwość dostępu do nośników kopii zapasowych, fizyczne ograniczenia pamięci oraz warunki umowy. Koordynator ISCP powinien odwoływać się do polityki odporności organizacji i BIA, aby pomóc w określeniu częstotliwości testowania nośników kopii zapasowych. Każda taśma zapasowa, kaseta lub dysk powinny być jednoznacznie oznakowane, aby zapewnić szybką identyfikację wymaganych danych w nagłych wypadkach. Wymaga to od organizacji opracowania skutecznej strategii znakowania i śledzenia mediów.

Zapasowe miejsca przetwarzania zapewniają organizacji lokalizację do wznowienia działania systemu w przypadku katastroficznego zdarzenia, które wyłącza lub niszczy podstawową instalację systemu. Istnieją trzy podstawowe typy alternatywnych urządzeń przetwarzających, odpowiadające poziomowi gotowości do działania jako ośrodek operacyjny systemu.

- **Zimne zapasowe miejsce pracy / przetwarzania** (*ang. Cold Site*). Zimne zapasowe miejsca pracy to lokalizacje, w których dostępna jest podstawowa infrastruktura i kontrola środowiskowa (np. zasilanie elektryczne i HVAC), ale nie ustanowiono ani nie zainstalowano sprzętu komputerowego ani telekomunikacyjnego. Jest wystarczająco dużo miejsca, aby pomieścić potrzebny sprzęt do utrzymania kluczowych funkcji systemu. Przykłady zimnych zapasowych miejsc pracy obejmują

nieużywane obszary centrum danych i nieużywaną powierzchnię biurową (jeśli nie są wymagane specjalistyczne środowiska centrum danych). Zimne zapasowe miejsce pracy są zwykle najtańszym alternatywnym rozwiązaniem dla miejsc przetwarzania, ponieważ pierwotnymi kosztami są jedynie dzierżawa lub utrzymanie wymaganych powierzchni do celów odzyskiwania. Czas odzyskiwania jest jednak najdłuższy, ponieważ cały sprzęt systemowy (w tym telekomunikacyjny) będzie musiał zostać zakupiony, zainstalowany, przetestowany, a oprogramowanie z kopii zapasowej oraz dane załadowane i przetestowane, zanim system będzie mógł działać. W zależności od wielkości i złożoności systemu odzyskiwanie może potrwać kilka dni lub tygodni.

- **Ciepłe zapasowe miejsca pracy / przetwarzania** (*ang. Warm Site*). Ciepłe zapasowe miejsca pracy to lokalizacje, które mają podstawową infrastrukturę miejsc zimnych, ale mają również zainstalowane wystarczające wyposażenie IT i telekomunikacyjne, aby obsługiwać odzyskiwany system. Jednak sprzęt nie jest załadowany oprogramowaniem ani danymi wymaganymi do obsługi systemu. Ciepłe zapasowe miejsca pracy powinny mieć czytniki nośników kopii zapasowych zgodne ze strategią tworzenia kopii zapasowych w systemie. Ciepłe zapasowe miejsca pracy mogą nie mieć sprzętu do uruchamiania wszystkich systemów lub wszystkich elementów systemu, ale wystarczą do obsługi kluczowych procesów biznesowych. Przykładem ciepłego zapasowego miejsca pracy jest system testowy lub deweloperski, który jest geograficznie oddzielony od systemu produkcyjnego. Sprzęt może być zainstalowany na miejscu do obsługi systemu, ale wymagałby powrotu do wersji produkcyjnej oprogramowania, załadowania danych z nośników kopii zapasowych i nawiązania komunikacji z użytkownikami. Innym przykładem jest dostępny sprzęt w alternatywnym obiekcie, w którym działają systemy niekrytyczne i który może zostać przekształcony w system krytyczny podczas zdarzenia awaryjnego. Ciepłe zapasowe miejsce pracy jest droższe niż miejsce zimne, ponieważ sprzęt jest już zakupiony i utrzymywany w tym miejscu, łącznie z uruchomionymi usługami telekomunikacyjnymi. Niektóre koszty mogą zostać zrekompensowane poprzez użycie sprzętu do funkcji niekrytycznych lub testowania. Odzyskiwanie w ciepłym

zapasowym miejscu pracy może potrwać od kilku godzin do kilku dni, w zależności od złożoności systemu i ilości danych do przywrócenia.

- **Gorące zapasowe miejsca pracy / przetwarzania** (*ang. Hot Site*). Gorące lokalizacje to lokalizacje z całkowicie sprawnym sprzętem i zdolnością do szybkiego przejęcia operacji systemu po utracie zdolności funkcjonowania instalacji podstawowej. Gorące zapasowe miejsca pracy ma wystarczającą ilość sprzętu i zainstalowaną najnowszą wersję oprogramowania produkcyjnego oraz wystarczająco pamięci do przechowywania danych systemu produkcyjnego. W gorących zapasowych miejscach pracy powinna być załadowana najnowsza wersja danych z kopii zapasowej, wymagająca tylko aktualizacji danych z ostatniej kopii zapasowej. W wielu przypadkach bazy danych oraz inne informacje zawarte w miejscach gorących są aktualizowane jednocześnie z głównymi bazami danych lub wkrótce po nich (replikacja synchroniczna i asynchroniczna). W gorących zapasowych miejscach pracy powinno być zapewnione szybkie przeniesienie łączności użytkowników systemu z miejsca głównego. Jednym z przykładów miejsca gorącego są dwa identyczne systemy produkcyjne w alternatywnych lokalizacjach, obsługujące różne lokalizacje geograficzne lub równoważące obciążenie produkcyjne. Każda lokalizacja jest zdolna do obsługi pełnego obciążenia, a dane są stale synchronizowane między systemami. Jest to najdroższa opcja, wymagająca pełnego działania systemu w alternatywnej lokalizacji i całej pojemności telekomunikacyjnej, z możliwością utrzymania lub szybkiej aktualizacji danych operacyjnych i baz danych wymagających również wsparcia operacyjnego równoważnego produkcji.

W celu ustalenia, jaki rodzaj miejsca odzyskiwania jest potrzebny, Koordynator ISCP powinien wziąć pod uwagę informacje dostarczone w BIA, aby ustalić jakie krytyczne procesy biznesowe są obsługiwane przez system, jakie jest ich MTD oraz jaki jest wpływ utraty systemu na biznes. Strategia odzyskiwania systemu informatycznego może obejmować jeden lub kilka alternatywnych rozwiązań przywrócenia przetwarzania. Na przykład niektóre funkcje systemu mogą być bardzo krytyczne i wymagać gorącego zapasowego miejsca przetwarzania, aby zminimalizować przestoje i wpływ na procesy biznesu. Jednak inne

funkcje tego samego systemu, takie jak proces raportowania lub drukowania wsadowego, mogą być niedostępne przez kilka dni, przy niewielkim wpływie i mogą być odtworzone po zakupie niezbędnego wyposażenia.

### 5.1.6 WYKORZYSTANIE PROCESÓW WYSOKIEJ DOSTĘPNOŚCI (HA)

HA to proces, w którym nadmiarowość i przełączanie awaryjne są wbudowane w system, tak aby zmaksymalizować jego dostępność. Koncepcja HA polega na osiągnięciu czasu sprawności wynoszącego 99,999 % lub więcej, co odpowiada zaledwie kilku minutom przestoju w roku.

HA może być kosztowną opcją dla systemów ze zduplikowanym sprzętem i specjalnym oprogramowaniem przełączania awaryjnego w celu wyeliminowania dowolnego pojedynczego punktu awarii. Zwykle z systemami HA wiążą się wyższe koszty utrzymania i wymagania dotyczące wsparcia. Dlatego HA nie jest opłacalną opcją dla wielu systemów i należy ją brać pod uwagę tylko w tych systemach, w których przestoje są nietolerowane. Przykładami mogą być systemy ruchu lotniczego i systemy finansowe. Ponadto systemy HA nie mogą zastąpić solidnej strategii tworzenia kopii zapasowych, ponieważ uszkodzenie danych w systemie może rozprzestrzeniać się poprzez system HA, co czyni system bezużytecznym. Bez kopii zapasowej systemu, odseparowanej od samego systemu, odzyskiwanie może być niemożliwe.

HA można wdrożyć w jednym miejscu, przy czym cała nadmiarowość systemu znajduje się w tym miejscu. Dzięki temu system będzie działał na poziomie HA, o ile nie nastąpi przerwa w obiekcie, w którym znajduje się system. Jednak przy wdrażaniu produktów lub usług HA w systemie, koordynator ISCP powinien rozszerzyć procesy HA na inne miejsca. Należy wziąć pod uwagę mechanizmy takie jak tworzenie kopii lustrzanych bloków w alternatywnej lokalizacji w celu zapewnienia redundancji i tworzenia kopii zapasowych danych systemowych poza obiektem systemowym. Ilekroć zapis jest wykonywany w bloku na podstawowym urządzeniu pamięciowym, ten sam zapis jest dokonywany na alternatywnym urządzeniu pamięci, w tym samym systemie pamięci lub między oddzielnymi systemami pamięci, w różnych lokalizacjach.

## 5.2 SYSTEMY TYPU KLIENT/SERWER

Systemy klient / serwer mogą mieć przetwarzanie i gromadzenie danych zarówno na poziomie serwera, jak i stacji roboczej klienta. Stacje robocze klientów są zwykle komputerami stacjonarnymi, chociaż coraz częściej jako klienci wykorzystywane są urządzenia mobilne. Urządzenia mobilne obejmują laptopy, tablety i smartfony oraz specjalistyczny sprzęt, taki jak czytniki kodów kreskowych QR i inne.

Postęp technologii bezprzewodowych i smartfonów umożliwiły użytkownikom dostęp do kluczowych funkcji serwera i usług, takich jak poczta e-mail, z ich telefonów komórkowych. Zwykle odbywa się to za pomocą zastrzeżonego oprogramowania innej firmy, które ustanawia komunikację i transfer danych do i z telefonu za pośrednictwem sieci dostarczanej przez operatorów sieci komórkowych.

Serwery obsługują udostępnianie i przechowywanie plików, przetwarzanie danych, centralny hosting aplikacji (np. e-mail lub centralną bazę danych), drukowanie, kontrolę dostępu, uwierzytelnianie użytkowników, łączność zdalnego dostępu i inne wspólne usługi systemowe. Lokalni użytkownicy, aby uzyskać dostęp do zasobów udostępnianych przez serwer, logują się na serwerze za pośrednictwem komputerów klienckich podłączonych do sieci.

### 5.2.1 UWAGI DOTYCZĄCE AWARYJNOŚCI SYSTEMÓW KLIENT / SERWER

Zagadnienia procedur awaryjnych dla systemów klient / serwer powinny kłaść nacisk na dostępność danych, poufność i integralność zarówno na poziomie systemu serwerowego, jak i na poziomie klienta. Aby spełnić te wymagania, należy regularnie wykonywać kopie zapasowe danych. W szczególności administrator systemu powinien rozważyć każdą z następujących praktyk dotyczących systemów klient / serwer:

- Przechowuj kopie zapasowe poza siedzibą lub w innej lokalizacji. Jak wspomniano w sekcji 3.4.2, nośniki kopii zapasowych powinny być przechowywane poza siedzibą lub w innym miejscu w obiekcie bezpiecznym, kontrolowanym środowiskowo.

- Standaryzuj sprzęt, oprogramowanie i urządzenia peryferyjne. Odzyskiwanie systemu jest szybsze, jeśli sprzęt, oprogramowanie i urządzenia peryferyjne są znormalizowane w całej organizacji. Ponadto krytyczne komponenty sprzętowe, które należy natychmiast odzyskać w razie awarii, powinny być kompatybilne z gotowymi komponentami komputerowymi dostępnymi na rynku. Ta zgodność pozwoli uniknąć opóźnień w zamawianiu niestandardowego sprzętu od dostawcy.
- Dokumentuj konfiguracje systemu i informacje o dostawcach. Dobrze udokumentowane konfiguracje systemu ułatwiają odzyskiwanie. Nazwy dostawców i informacje kontaktowe do nich, którzy na wypadek awarii dostarczą niezbędny sprzęt, oprogramowanie i inne komponenty, powinny być wymienione w planie awaryjnym, tak aby można było szybko kupić komponenty zamienne.
- Koordynuj zasady bezpieczeństwa i zabezpieczenia systemu. Rozwiązania awaryjne klient / serwer powinny być skoordynowane z politykami bezpieczeństwa i zabezpieczeniami systemu. Wybierając odpowiednie techniczne rozwiązanie awaryjne, zastosuj podobne rozwiązania w zakresie zabezpieczeń i działań związanych z bezpieczeństwem (np. ocena ryzyka, skanowanie podatności) jak stosowane w systemie produkcyjnym, tak aby zapewnić, że rozwiązanie awaryjne nie naruszy ani nie ujawni wrażliwych danych podczas awarii system .
- Wykorzystaj wyniki z BIA. Powiązania pomiędzy systemami uwidocznione za pośrednictwem BIA powinny mieć odzwierciedlenie w rozwiązaniu awaryjnym.

Dodatkowe uwagi dotyczące komputerów klienckich obejmują:

- Zminimalizuj ilość danych przechowywanych na komputerze klienckim. Krytyczne dane użytkownika powinny być przechowywane na serwerach centralnych, których kopie zapasowe są tworzone w ramach korporacyjnej strategii tworzenia kopii zapasowych, a nie na dysku twardym komputera klienckiego.
- Zautomatyzuj tworzenie kopii zapasowych danych. Systemy klient / serwer powinny mieć zainstalowane oprogramowanie, które automatycznie planuje tworzenie kopii zapasowych danych w centralnej lokalizacji kopii danych zapasowych. Dane do

tworzenia kopii zapasowych powinny być przechowywane pod wspólną nazwą katalogu (np. \ Moje dokumenty), aby ułatwić automatyczne tworzenie kopii zapasowych i upewnić się, że kopia zapasowa dotyczy tylko odpowiednich danych. Jeśli proces tworzenia kopii zapasowej systemu klienta nie jest zautomatyzowany, należy zachęcać użytkowników do regularnego tworzenia kopii zapasowych danych. W miarę możliwości należy skonfigurować automatyczne harmonogramy tworzenia kopii zapasowych dla autonomicznych komputerów stacjonarnych i urządzeń przenośnych.

- Podaj wskazówki dotyczące zapisywania danych na komputerach klienckich. Poinstruowanie użytkowników, aby zapisywali dane w określonym folderze na komputerze, zmniejsza obciążenie działu obsługi klienta IT. Jeśli komputer musi zostać przebudowany, technik działu IT będzie wiedział, które foldery skopiować i zachować podczas odzyskiwania.
- Przechowuj informacje o kopii zapasowej w alternatywnej lokalizacji. Jeśli użytkownicy wykonują kopię zapasową danych w autonomicznym systemie zamiast zapisywać dane w sieci, należy zapewnić środki do przechowywania nośników w alternatywnej lokalizacji. Licencje na oprogramowanie i oryginalne oprogramowanie systemowe, umowy SLA i umowy z dostawcami oraz inne ważne dokumenty dotyczące samodzielnego oprogramowania, powinny być przechowywane wraz z nośnikiem kopii zapasowej. Miejsce przechowywania powinno znajdować się wystarczająco daleko od pierwotnego miejsca, aby zmniejszyć prawdopodobieństwo, że oba ośrodki zostaną dotknięte tym samym zdarzeniem awaryjnym.

Aspekty awaryjne dotyczące serwerów w systemie klient / serwer odnoszą się w dużej mierze do łączności LAN i WAN w celu komunikowania się ze swoimi klientami. Z tego powodu komponenty serwera muszą uwzględniać środki awaryjne systemu podobne do tych stosowanych w sieciach LAN i WAN.

- Standaryzacja sprzętu, oprogramowania i urządzeń peryferyjnych. Odzyskiwanie systemu może zostać przyspieszone, jeśli sprzęt, oprogramowanie i urządzenia peryferyjne są znormalizowane w całym systemie klient / serwer. Koszty odzyskiwania można zmniejszyć, ponieważ można wyznaczyć standardowe konfiguracje i udostępnić zasoby. Standaryzowane komponenty zmniejszają również koszty utrzymania systemu w całej organizacji.
- Dokumentowanie konfiguracji i dostawców. Dokumentuj architekturę serwera i konfiguracje jego różnych komponentów. Ponadto plan awaryjny powinien określać specyfikacje dostawców i modeli, aby ułatwić szybką wymianę sprzętu po zakłóceniu.
- Rozwiązania awaryjne serwera powinny być skoordynowane z polityką bezpieczeństwa sieci, w której podobne środki bezpieczeństwa i działania związane z bezpieczeństwem (np. ocena ryzyka, skanowanie podatności) w środowisku produkcyjnym powinny być wdrażane w rozwiązaniu awaryjnym, aby zapewnić, że podczas awarii systemu, wykonanie technicznych rozwiązań awaryjnych nie naraża ani nie ujawnia wrażliwych danych. Bezpieczeństwo danych w systemie klient / serwer ma kluczowe znaczenie, ponieważ większość systemów jest wielodostępowa, z wieloma użytkownikami i aplikacjami rezydującymi w tym samym systemie, o różnych wymaganiach bezpieczeństwa i zabezpieczeń.
- Koordynacja rozwiązań awaryjnych z procedurami reagowania na incydenty cyberbezpieczeństwa. Ponieważ wiele organizacji korzysta z rozwiązań typu Web do prezentowania swojego wizerunku, uszkodzenie w tym obszarze może niekorzystnie odbić się na reputacji organizacji. Aby ograniczyć konsekwencje takiego ataku, rozwiązania awaryjne powinny być ściśle koordynowane z procedurami reagowania na incydenty cyberbezpieczeństwa, mającymi na celu ograniczenie skutków cyberataku.
- Wykorzystanie wyników z BIA. Wpływy i priorytety powiązań sieci LAN lub WAN wynikające z BIA, powinny zostać uwzględnione w celu ustalenia wymagań i priorytetów odzyskiwania

### 5.2.2 ROZWIĄZANIA AWARYJNE W OBSZARZE SYSTEMÓW KLIENT / SERWER

W systemach typu klient / serwer dostępna jest szeroka gama technicznych rozwiązań awaryjnych. W tej sekcji omówiono kilka skutecznych i sprawdzonych praktyk.

Szyfrowanie to popularne narzędzie bezpieczeństwa stosowane na urządzeniach klienckich. Przy zwiększonym wykorzystaniu podpisów elektronicznych w celu zapewnienia niezaprzeczalności i stosowaniu szyfrowania w celu zachowania poufności i / lub integralności, organizacje powinny rozważyć włączenie szyfrowania do swojej strategii tworzenia kopii zapasowych. Należy również rozważyć szyfrowanie nośników kopii zapasowych, przekazywanych poza miejsce przechowywania, w celu zabezpieczenia danych w przypadku ich utraty lub kradzieży na trasie lub w innej lokalizacji.

Jeśli zaszyfrowane dane są wysyłane poza miejsce przechowywania, powinien istnieć system zarządzania kluczami kryptograficznymi, tak aby upewnić się, że dane są czytelne gdy zajdzie potrzeba ich odzyskania w nowym systemie. Zarówno klucze kryptograficzne, jak i oprogramowanie do szyfrowania muszą być dostępne w nowym systemie. Istotnymi materiałami kryptograficznymi są klucze i punkty inicjujące szyfrowanie, używane do ustalenia i utrzymania parametrów szyfrowania. Istotne materiały kryptograficzne powinny być przechowywać w centralnej lokalizacji (w taki sam sposób jak inne materiały kryptograficzne używane w organizacji) lub na nośniku wymiennym, oddzielnie od samego nośnika kopii zapasowej.

Kopie zapasowe danych systemowych klient / serwer można wykonać na różne sposoby, w tym wymienione poniżej.

- **Cyfrowy dysk wideo (DVD).** Dyski DVD są tanim nośnikiem pamięci i mają pojemność około 4,7 gigabajtów (GB). Do odczytu z DVD-ROM wystarczy menedżer plików systemu operacyjnego; do zapisu na DVD-ROM wymagany jest odpowiedni napęd umożliwiający zapis oraz odpowiednie oprogramowanie.
- **Pamięć sieciowa**. Dane przechowywane w sieciowych systemach klient / serwer można wykonać na dysku sieciowym. Ilość danych, których kopię zapasową można wykonać z systemu klient / serwer, jest ograniczona pojemnością dysku sieciowego

lub alokacją dysku dla konkretnego użytkownika. Jeśli użytkownicy zostaną poinstruowani, aby zapisać pliki na dysku sieciowym, należy wykonać kopię zapasową samego dysku sieciowego za pośrednictwem programu do tworzenia kopii zapasowych sieci lub serwera. Typowe rodzaje architektury sieciowej pamięci masowej obejmują pamięci masowe typu NAS i sieciowe pamięci masowe typu SAN. Systemy pamięci masowej zawierają rozwiązania zapewniające redundancję i korektę błędów i można je skonfigurować tak, aby utrzymywały nadmiarowość w kilku lokalizacjach.

- **Zewnętrzne dyski twarde**. Replikacja danych lub synchronizacja z zewnętrznym dyskiem twardym jest powszechną metodą tworzenia kopii zapasowych komputerów stacjonarnych i urządzeń mobilnych. Urządzenia te można podłączyć do zewnętrznego dysku twardego i powielać pożądane dane z urządzenia na zewnętrzny dysk twardy. Wiele zewnętrznych dysków twardych zawiera oprogramowanie do tworzenia kopii zapasowych, które można wykorzystać do tworzenia kopii zapasowych dysków podstawowych.
- **Internetowa kopia zapasowa (kopia w chmurze obliczeniowej)**. Internet Backup, Online lub Cloud Backup to usługa komercyjna, która umożliwia użytkownikom komputerów stacjonarnych i urządzeń mobilnych tworzenie za opłatą kopii zapasowych danych w zdalnej lokalizacji przez Internet. Na komputerze stacjonarnym lub urządzeniu mobilnym zainstalowane jest narzędzie, które pozwala użytkownikowi planować tworzenie kopii zapasowych, wybierać pliki i foldery, których kopie zapasowe mają zostać utworzone, oraz ustanawiać schemat archiwizacji, aby zapobiec zastępowaniu plików. Dane mogą być szyfrowane na czas transmisji, utrudnia to jednak przesyłanie danych. Zaletą Internet Backup jest to, że użytkownik nie musi kupować sprzętu ani nośników do tworzenia kopii zapasowych danych i że dane są łatwo dostępne do pobrania w celu odzyskania w sytuacji awaryjnej.

Serwery zwykle mają znacznie większe ilości danych, które muszą być utrzymywane i zabezpieczane. Zaleca się w środowiskach z wieloma serwerami, aby pamięć nie była dedykowana dla każdego serwera, ale raczej scentralizowana do użytku przez wiele

serwerów. SAN i NAS są popularnymi wieloserwerowymi systemami pamięci. Centralizacja danych wielu serwerów pozwala na wspólne tworzenie kopii zapasowych danych do przechowywania poza siedzibą. Biorąc pod uwagę dużą ilość danych, dla których należy wykonać kopię zapasową, zaleca się stosowanie oddzielnej i dedykowanej sieci tylko do przesyłania danych wymaganych do utworzenia zapasowej kopii danych. Umożliwi to przeznaczenie sieci podstawowej na ruch produkcyjny i nie wpłynie na proces tworzenia kopii zapasowej.

Rozwiązania awaryjne powinny być wbudowane w system klient / serwer podczas projektowania i wdrażania. Na przykład system klient / serwer może być skonstruowany w taki sposób, że wszystkie dane znajdują się w jednej lokalizacji (np. w głównej siedzibie organizacji) i są replikowane lokalnie. Dane z jednej lokalizacji można replikować do drugiej. Oznacza to, że każda z lokalizacji działa jako kopia zapasowa dla drugiej.

Jak pokazuje powyższy przykład, system klient / serwer zazwyczaj zapewnia pewien nieodłączny poziom nadmiarowości, który można włączyć do strategii awaryjnej. Rozważmy na przykład krytyczny system, który jest rozproszony między centralą organizacji, a małym biurem. Zakładając, że dane są replikowane w obu lokalizacjach, opłacalną strategią odzyskiwania może być ustanowienie wzajemnego porozumienia między tymi dwoma lokalizacjami. Zgodnie z tą umową, w przypadku zakłóceń w jednym biurze, niezbędny personel przeniesie się do drugiego biura, aby kontynuować przetwarzanie zgodnie z funkcjami systemu. Strategia ta pozwala zaoszczędzić znaczne nieprzewidziane koszty, unikając konieczności zamawiania i wyposażania alternatywnych lokalizacji.

Koordynator ISCP rozważając wykorzystanie zdalnych miejsc pracy do tworzenia kopii zapasowych systemu, korzystanie z Internetu lub innych środków tworzenia kopii zapasowych, powinien zapewnić, że zdalnie hostowane usługi pamięci masowej mogą zapewnić taki sam poziom ochrony danych jak miejsce ich podstawowego przetwarzania. Można tego dokonać poprzez umowy SLA oraz okresowe przeglądy i oceny zdalnych magazynów.

## 5.3 SYSTEMY TELEKOMUNIKACYJNE

Istnieją dwie podstawowe klasy systemów telekomunikacyjnych: sieci LAN i WAN. Łączność bezprzewodowa, powszechna w urządzeniach mobilnych, może być używana zarówno w środowiskach LAN lub WAN.

Sieć LAN znajduje się w środowisku biurowym. Mogą to być dwa komputery PC podłączone do jednego przełącznika sieciowego lub może obsługiwać setki użytkowników i wiele serwerów. Sieci LAN można rozwijać przy użyciu dowolnej z kilku topologii. Każde połączenie w sieci LAN jest uważane za węzeł.

WAN to sieć transmisji danych, która polega na połączeniu dwóch lub więcej systemów rozproszonych na dużym obszarze geograficznym. Łącza komunikacyjne, zwykle dostarczane przez operatora publicznego, zapewniają połączenie umożliwiające jednemu systemowi interakcję z innymi systemami.

Sieci WAN mogą łączyć ze sobą sieci LAN, łączyć się z systemami klasy mainframe i łączyć komputery klienckie z serwerami. Sieci WAN spełniają wiele wymagań komunikacyjnych w rozproszonych geograficznie środowiskach. Łącza komunikacyjne WAN obejmują następujące metody zestawiania połączeń.

- **E-1**. E-1 to dedykowane łącze telekomunikacyjne obsługujące szybkość transmisji danych 2048 kilobitów na sekundę (kbps). Linia E-1 składa się z 32 pojedynczych kanałów 64 kb/s, z czego 31 kanałów może być skonfigurowany do przesyłania sygnałów głosowych lub danych (pierwszy przedział [timeslot 0, TS0] nie jest używany do przesyłania danych, przesyłane są nim bity służące m.in. synchronizacji). Strukturalne łącza komunikacyjne E-1 są stosowane, gdy wymagane są wielokrotności linii 64 kb/s.
- **E-3**. E-3 to dedykowane łącze telekomunikacyjne obsługujące prędkości transmisji 34 368 Mb/ s. Linia E-3 składa się z 16 łączy E1 (512 pojedynczych kanałów 64 kb/s).
- **Frame Relay**. Frame Relay to sieć z komutacją pakietów, używana do łączenia odległych sieci lokalnych (LAN), przesyłania danych, obrazu i głosu oraz dostępu

do Internetu. W tej technice informacja jest dzielona na ramki o zmiennej długości, które przenoszą dane między sieciami LAN, co pozwala na przekazywanie informacji między urządzeniami końcowymi sieci rozległych (WAN).

- **ATM** (*ang. Asynchronous Transfer Mode*) jest szerokopasmową technologią komunikacji asynchronicznej, która wykorzystywana jest do przesyłania danych interakcyjnych, różnej wielkości plików, transmisji głosu, a także sygnału wizyjnego. Standard ATM może być stosowany zarówno w sieciach lokalnych LAN, miejskich MAN jak i rozległych WAN. Połączenie pomiędzy odbiorcą a nadawcą, tworzone jest na podstawie informacji zawartej w przesyłanych komórkach informacyjnych (*ang. cell*) o jednakowych rozmiarach.
- **SDH (***ang. Synchronous Digital Hierarchy***)**, czyli Synchroniczna Hierarchia Systemów Cyfrowych. Jest to technologia sieci transportu informacji, charakteryzująca się tym, że wszystkie urządzenia działające w sieci SDH, pracujące w trybie bezawaryjnym, są zsynchronizowane zarówno do nadrzędnego zegara (PRC) jak i do siebie nawzajem (w odróżnieniu od takich technologii jak, np. ATM). Ważną cechą jest również to, że podstawowa jednostka transportowa STM-*n* (*ang. Synchronous Transport Module* - Synchroniczny Moduł Transportowy) w czasie zwielokrotniania ma przepływność, będącą *n*-tą wielokrotnością STM-1 (STM-1 = 155,52 Mb/s). Ta właściwość nie występuje np. w technologii PDH.

Wymienione rodzaje łączy telekomunikacyjnych są podane jako przykład. W rzeczywistości, wraz z rozwojem technologii telekomunikacyjnej mogą występować inne rodzaje łączy.

### 5.3.1 UWAGI DOTYCZĄCE SYTUACJI AWARYJNYCH W SIECIACH TELEKOMUNIKACYJNYCH

Opracowując strategię odzyskiwania usług telekomunikacyjnych, Koordynator ISCP powinien zastosować uwagi podane w Sekcji 5.2.1 dotyczące systemów klient / serwer. Ponadto należy wziąć pod uwagę następujące praktyki:

- **Dokumentacja telekomunikacyjna**. Fizyczne i logiczne schematy sieci telekomunikacyjnej powinny być aktualne. Schemat fizyczny sieci powinien przedstawiać fizyczny układ obiektu, w którym znajduje się sieć LAN i / lub WAN,

a numery gniazd kabli powinny być udokumentowane na schemacie fizycznym. Schematy powinny również identyfikować urządzenia sieciowe, adresy IP, nazwy DNS i typy łączy komunikacyjnych oraz dostawców. Schemat logiczny sieci powinien przedstawiać infrastrukturę telekomunikacyjną i jej węzły. Oprogramowanie do inwentaryzacji sieci może zapewnić dokładny obraz środowiska telekomunikacyjnego. Oba schematy pomagają personelowi odpowiedzialnemu za odzyskiwanie danych zidentyfikować miejsce wystąpienia problemów i szybciej przywrócić usługi telekomunikacyjne.

- **Dokumentacja konfiguracji systemu i informacje o dostawcach**. Dokumentuj konfiguracje sieciowych urządzeń łączących, które ułatwiają komunikację (np. rutery, przełączniki, mosty i koncentratory) w celu ułatwienia odzyskiwania. Dostawcy i ich dane kontaktowe powinny być udokumentowane w planie awaryjnym, aby zapewnić szybką naprawę lub wymianę sprzętu i oprogramowania. Plan powinien również dokumentować dostawców usług telekomunikacyjnych, w tym informacje dotyczące PoC oraz informacji umownych w zakresie SLA.
- **Koordynacja z politykami bezpieczeństwa i zabezpieczeniami**. Awaryjne rozwiązania telekomunikacyjne powinny być skoordynowane z polityką bezpieczeństwa. Dlatego przy wyborze odpowiednich technicznych rozwiązań w zakresie awaryjnym związanym z telekomunikacją, należy przyjąć podobne rozwiązania w odniesieniu do zabezpieczeń jak w systemach podstawowych, tak aby podczas awarii sieci podstawowej rozwiązania w zakresie awaryjnym nie spowodowało narażenia wrażliwych danych na ujawnienie.
- **Wykorzystanie wyników z BIA**. Oddziaływania i priorytety wykazane w BIA dotyczące współpracujących systemów powinny zostać poddane przeglądowi w celu ustalenia priorytetów odzyskiwania usług telekomunikacyjnych. BIA powinna zidentyfikować poziomy wpływu NSC 199 w zakresie wysokiej dostępności dla połączeń sieciowych, które obsługują misję COOP, funkcje podstawowe lub podstawowe funkcje krajowe.

### 5.3.2 ROZWIĄZANIA AWARYJNE W TELEKOMUNIKACJI

Chociaż podobne systemy występują zarówno w systemach telekomunikacyjnych LAN, jak i WAN, istnieją różne strategie i rozwiązania, które Koordynator ISCP powinien wziąć pod uwagę przy określaniu ogólnej strategii odzyskiwania usług telekomunikacyjnych. Różnice w rozwiązaniach istnieją przede wszystkim ze względu na właściwość geograficzną. Podczas gdy sieci LAN są zwykle zaimplementowane na małych obszarach (biura lub kampusy), a routing i okablowanie są własnością organizacji lub są przez nią zarządzane, sieci WAN zazwyczaj opierają się na operatorach sieci telekomunikacyjnych (NSP), zarówno w zakresie routingu, jak i okablowania.

Opracowując ISCP dla sieci LAN, koordynator ISCP powinien zidentyfikować pojedyncze punkty awarii, które wpływają na krytyczne systemy lub procesy opisane w BIA. Analiza ta może obejmować zagrożenia dla systemu okablowania, takie jak przecięcia kabli, zakłócenia elektromagnetyczne oraz uszkodzenia wynikające z pożaru, zalania i innych zagrożeń. Jako zabezpieczenie można w razie potrzeby zainstalować kable nadmiarowe. Na przykład instalacja duplikatów kabli do komputerów może nie być opłacalna. Jednak rentowne może być zainstalowanie dodatkowego kabla gigabitowego między piętrami, aby hosty na obu piętrach mogły zostać ponownie podłączone, gdyby główny kabel został przecięty.

Planowanie awaryjne powinno również uwzględniać urządzenia łączące sieć, takie jak koncentratory, przełączniki, rutery i mostki sieciowe. BIA powinien scharakteryzować role, jakie każde urządzenie pełni w sieci, a dla każdego urządzenia należy opracować rozwiązanie awaryjne w oparciu o krytyczność BIA. Jako przykład strategii awaryjnej dla urządzeń łączących sieć należy wymienić nadmiarowe inteligentne routery sieciowe, które mogą być zainstalowane w sieci, umożliwiając ruterowi przejęcie pełnego obciążenia pracą, jeśli inny ruter ulegnie awarii.

Zdalny dostęp to usługa świadczona przez serwery i urządzenia w sieci LAN. Zdalny dostęp zapewnia wygodę użytkownikom pracującym poza siedzibą lub umożliwia komunikację między serwerami. Zdalny dostęp może być przeprowadzany różnymi metodami, przede wszystkim za pośrednictwem wirtualnej sieci prywatnej (VPN). Jeśli wystąpi awaria lub

poważne zakłócenie systemu, dostęp zdalny może służyć jako rozwiązanie awaryjne, zapewniając zespołom odzyskiwania lub użytkownikom z innej lokalizacji dostęp do danych dotyczących całej organizacji. Jeśli dostęp zdalny zostanie ustanowiony jako strategia awaryjna, należy określić wymagania dotyczące przepustowości danych i wykorzystać je do skalowania rozwiązania dostępu zdalnego. Ponadto należy wdrożyć zabezpieczenia, takie jak uwierzytelnianie wieloskładnikowe MFA i szyfrowanie danych, jeśli komunikacja zawiera informacje o umiarkowanym lub dużym wpływie wg. NSC 199. Dostęp zdalny działa tylko wtedy, gdy serwer dostępu zdalnego i sieć działają zarówno w głównej, jak i alternatywnej lokalizacji.

Bezprzewodowe sieci lokalne (np. WiFi) mogą służyć jako skuteczne rozwiązanie awaryjne do przywracania usług sieciowych po zakłóceniu przewodowej sieci LAN. Sieci bezprzewodowe nie wymagają infrastruktury okablowania konwencjonalnych sieci LAN, dlatego mogą być szybko instalowane jako rozwiązanie tymczasowe lub trwałe. Jednak sieci bezprzewodowe używają sygnałów radiowych, umożliwiając przechwycenie danych. Jeśli ruch komunikacyjny zawiera informacje o umiarkowanym lub dużym wpływie według NSC 199, podczas wdrażania sieci bezprzewodowej należy zastosować zabezpieczenia, takie jak szyfrowanie danych. Bezprzewodowe sieci LAN umożliwiają szybki tymczasowy dostęp do urządzeń mobilnych, które zwykle mają wbudowane rozwiązania umożliwiające łączność bezprzewodową. Routery bezprzewodowe, jako funkcje standardowe, zapewniają uwierzytelnianie hasłem i szyfrowanie transmisji.

W przypadku organizacji rozważających łączność zdalną należy zaimplementować kilka wymagań i wytycznych dotyczących bezpieczeństwa. Obejmuje to weryfikację tożsamości użytkownika za pomocą uwierzytelnienia elektronicznego. Wytyczne dotyczące uwierzytelnienia elektronicznego zapewniają cztery podstawowe poziomy ochrony, od minimalnej weryfikacji tożsamości (poziom 1) do kryptograficznych kluczy uwierzytelniania dwuskładnikowego (poziom 4).

Rozwiązania awaryjne WAN obejmują wszystkie omówione środki dla systemów klient / serwer i sieci LAN. Ponadto planowanie awaryjne sieci WAN musi uwzględniać łącza komunikacyjne łączące różne systemy. Na strategie awaryjne WAN ma wpływ rodzaj danych

przesyłanych w sieci. Sieć WAN obsługująca system o znaczeniu krytycznym (patrz punkt 5.4) może wymagać bardziej niezawodnej strategii odzyskiwania niż sieć WAN, która łączy wiele sieci LAN w celu prostego udostępniania zasobów. Organizacje powinny rozważyć następujące rozwiązania awaryjne zapewniające dostępność sieci WAN:

- **Nadmiarowe łącza komunikacyjne**. Nadmiarowe łącza komunikacyjne są zwykle konieczne, gdy sieć przetwarza krytyczne dane. Łącze nadmiarowe może być tego samego typu, na przykład dwa połączenia E-1, lub łącze zapasowe może zapewniać zmniejszoną szerokość pasma, aby pomieścić tylko krytyczne transmisje w sytuacjach awaryjnych. Na przykład linia ISDN[9] (Integrated Services Digital Network) o przepustowości 128 Kb/s (2B+d) może być wykorzystana jako awaryjne łącze komunikacyjne dla podstawowego połączenia E-1. W przypadku korzystania z nadmiarowych łączy, koordynator ISCP powinien upewnić się, że łącza mają fizyczną separację i nie są zestawione tą samą drogą, w przeciwnym razie pojedynczy incydent, taki jak przecięcie kabla, może zakłócić oba łącza.
- **Nadmiarowi dostawcy usług sieciowych**. Jeśli wymagana jest prawie 100-procentowa łączność, nadmiarowe łącza komunikacyjne mogą być zapewnione przez wielu operatorów sieci telekomunikacyjnych (*ang. Network Service Provider – NSP*). W przypadku wybrania tego rozwiązania, Koordynator ISCP powinien dopilnować, aby infrastruktura nadmiarowych łączy nie współdzieliła wspólnych obiektów w żadnym punkcie, w tym wejść do budynków (miejsc, w których połączenie WAN kończy się w obiekcie).
- **Nadmiarowe urządzenia przełączające**. Zduplikowane urządzenia przełączające, takie jak routery, przełączniki i zapory sieciowe, mogą zapewnić wysoką dostępność w interfejsach LAN i zapewnić redundancję w przypadku awarii jednego urządzenia. Zduplikowane urządzenia zapewniają także równoważenie obciążenia w kierowaniu ruchem (routingu).

[9] ISDN jest technologią przestarzałą, a jej przytoczenie ma znaczenie jako przykład.

- **Redundancja po stronie operatora sieci telekomunikacyjnej (NSP) lub dostawcy usług internetowych (ISP)**. Koordynator ISCP powinien skonsultować się z wybranym NSP lub ISP, tak aby ocenić solidność i niezawodność w swoich sieciach rdzeniowych (np. nadmiarowe urządzenia przełączające i zabezpieczenia zasilania).

Szybkie wykrycie zakłóceń telekomunikacyjnych ograniczy ich skutki. Można tego dokonać poprzez zainstalowanie oprogramowania monitorującego. Jeśli węzeł lub połączenie obniża swoje parametry lub ulega awarii, oprogramowanie monitorujące wysyła alert. Oprogramowanie monitorujące może ułatwiać rozwiązywanie problemów i często wyświetla administratorowi ostrzeżenie, zanim użytkownicy zauważą problemy. Wiele rodzajów oprogramowania monitorującego może być skonfigurowanych do automatycznego wysyłania wiadomości do wyznaczonej osoby (osób) poprzez np. wiadomość SMS lub e-mail, gdy parametr systemu wykracza poza zakres specyfikacji.

Umowy SLA mogą ułatwić szybkie odzyskanie w przypadku problemów z oprogramowaniem lub sprzętem związanych z usługami telekomunikacyjnymi. Umowę SLA można również opracować z NSP lub ISP, tak aby zagwarantować pożądaną dostępność sieci i ustalić kary umowne, jeśli sieć dostawcy jest niedostępna. Jeśli dostawca usług sieciowych lub dostawca usług internetowych zawarł umowę o dostarczeniu urządzeń przełączających, takich jak routery, dostępność tych urządzeń należy uwzględnić w umowie SLA.

## 5.4 SYSTEMY KLASY MAINFRAME

W przeciwieństwie do architektury klient/serwer, architektura mainframe jest scentralizowana. Klienci, którzy uzyskują dostęp do komputera mainframe, są traktowani jak terminale bez możliwości przetwarzania lub przechowywania danych. Cała moc obliczeniowa dla systemu mieści się w samym komputerze mainframe. Terminale akceptują wyjście tylko z komputera głównego. Na początku terminale te składały się przede wszystkim z monitorów i klawiatur bez procesorów. Teraz jednak komputery mainframe zwykle nie mają tradycyjnych terminali. Zamiast tego komputery stacjonarne i przenośne uzyskują dostęp do komputerów mainframe za pomocą oprogramowania do emulacji terminali.

Komputer mainframe to komputer wielożytkownikowy, zaprojektowany w celu zaspokojenia potrzeb obliczeniowych dużej organizacji. Termin „mainframe” został stworzony, aby opisać duże komputery centralne opracowane pod koniec lat 50 i 60 dwudziestego wieku do pełnienia funkcji z zakresu księgowości i zarządzania informacjami. Systemy mainframe przechowują wszystkie dane w centralnej lokalizacji, a nie rozpraszają tych danych między wieloma komputerami.

### 5.4.1 ZAGADNIENIA ZWIĄZANE Z AWARIAMI KOMPUTERA MAINFRAME

Chociaż przetwarzanie na komputerze mainframe jest bardziej wydajne i scentralizowane niż na innych typach platform, ma wiele takich samych wymagań awaryjnych jak systemy typu klient/serwer. Ponieważ mainframe wykorzystuje scentralizowaną architekturę, mainframe nie ma integralnej nadmiarowości, jaką zapewnia rozproszony system lub sieć. W rezultacie dostępność komputerów mainframe i kopie zapasowe danych mają kluczowe znaczenie. Przy określaniu wymagań dotyczących awaryjności komputerów mainframe należy wziąć pod uwagę następujące środki:

- **Przechowuj nośniki kopii zapasowych poza siedzibą firmy**. Nośniki kopii zapasowych powinny być etykietowane, rejestrowane i przechowywane poza siedzibą organizacji w bezpiecznym, kontrolowanym środowisku. Miejsce przechowywania powinno znajdować się wystarczająco daleko od pierwotnego miejsca lokalizacji, aby zmniejszyć prawdopodobieństwo, że oba te miejsca dotknie to samo zdarzenie. Ponadto, w zależności od poziomu wpływu wg. NSC 199, może być konieczne szyfrowanie danych w celu ochrony informacji na kopii zapasowej systemu podczas transportu i składowania, aby zminimalizować ryzyko ujawnienia danych związane z utratą lub kradzieżą nośnika kopii zapasowej.
- **Dokumentuj konfiguracje systemu i dostawców**. Prowadzenie szczegółowej dokumentacji konfiguracji systemu zwiększa możliwości odzyskiwania systemu. Ponadto w planie awaryjnym należy zidentyfikować dostawców, którzy dostarczają niezbędny sprzęt, oprogramowanie i inne komponenty.

- **Koordynuj działania z polityką bezpieczeństwa sieci i zabezpieczeniami systemu**. Rozwiązania awaryjne na komputerach mainframe powinny obejmować powielanie interfejsów i infrastruktury telekomunikacyjnej, a także koordynację z politykami bezpieczeństwa sieci, takimi jak rygorystyczne kontrole dostępu.
- **Wykorzystaj wyniki z BIA**. Wpływy i priorytety powiązanych systemów wspierających w organizacji kluczowe zadania / procesy biznesowe zidentyfikowane przez BIA, powinny zostać poddane przeglądowi w celu ustalenia wymagań i priorytetów odzyskiwania.

### 5.4.2 ROZWIĄZANIA AWARYJNE NA KOMPUTERACH MAINFRAME

Systemy komputerowe mainframe wymagają odmiennej strategii awaryjnej niż systemy rozproszone, ponieważ dane są przechowywane w jednym miejscu. Strategie awaryjne powinny kłaść nacisk na aspekty związane z przechowywaniem danych na komputerach mainframe i z ich architekturą. Nadmiarowe komponenty systemu mają krytyczne znaczenie dla zapewnienia, że awaria komponentu systemu, takiego jak zasilacz, nie spowoduje awarii całego systemu. Należy również zastosować UPS i systemy monitorowania i zarządzania systemami zasilania, aby zapewnić, że wahania zasilania nie wpłyną na komputer mainframe. Ponieważ komputery mainframe zwykle przetwarzają duże krytyczne aplikacje, może być konieczne zastosowanie rozwiązania długoterminowego zasilania rezerwowego. Agregat prądotwórczy może zapewnić, że przetwarzanie na komputerze mainframe nie zostanie przerwane przez awarię zasilania.

Nadmiarowość dysku można zapewnić dla urządzeń pamięci masowej bezpośredniego dostępu (DASD) poprzez wdrożenie rozwiązania RAID.

Ponieważ każda architektura komputerów mainframe jest unikatowa i scentralizowana, strategią awaryjną jest udostępnienie systemu zastępczego w alternatywnym ciepłym lub gorącym miejscu przetwarzania. Ponieważ rezerwowe platformy mainframe są bardzo kosztowne w zakupie i utrzymaniu, wiele organizacji korzysta z usług komercyjnych. Organizacje zazwyczaj również utrzymują umowy wsparcia technicznego w celu naprawy uszkodzonych urządzeń. Jednak sama pomoc dostawcy może nie przywrócić funkcji systemu

w dopuszczalnym czasie przestoju. We wszystkich przypadkach umowy SLA dostawcy powinny być aktualizowane i sprawdzane, aby upewnić się, że dostawca zapewnia odpowiednie wsparcie w celu spełnienia wymagań dostępności systemu.

Tworzenie kopii zapasowych na komputerach mainframe powinno odbywać się regularnie, a nośniki kopii zapasowych powinny być przechowywane poza siedzibą. Harmonogramy tworzenia kopii zapasowych i przechowywania powinny opierać się na krytyczności przetwarzanych danych i częstotliwości ich modyfikacji (rozwiązania tworzenia kopii zapasowych znajdują się w Sekcji 5.2.2.). Podobnie jak w przypadku architektury klient/serwer, zdalne składowanie danych w zapasowym miejscu pracy może być skutecznym rozwiązaniem awaryjnym. Ponadto, w niektórych przypadkach można zastosować technologie replikacji dysków, wirtualizacji NAS lub SAN, które replikują różne platformy na jednym serwerze replikującym.

## 5.5 PODSUMOWANIE ZAGADNIEŃ PLANOWANIA AWARYJNEGO SYSTEMU

W przypadku planowania awaryjnego systemu informatycznego, koordynator ISCP powinien rozważyć środki techniczne wynikające z dwóch perspektyw planowania strategii odzyskiwania systemu:

- Czy aspekty awaryjne, uwzględniają wymagania techniczne oraz inne czynniki towarzyszące, oraz
- Czy rozwiązania wykorzystywane do wdrażania strategii awaryjnej posiadają wsparcie technicznie.

Tabela 5-1 zawiera podsumowanie rozważanych rozwiązań awaryjnych.

| Czynniki brane pod uwagę w zakresie rozwiązań awaryjne | Systemy klient/serwer | Systemy telekomunikacyjne | Systemy klasy mainframe |
|---|---|---|---|
| System dokumentów, konfiguracje i informacje o dostawcy | X | X | X |
| Zachęcanie użytkowników do tworzenia kopii zapasowych danych | X | | |
| Koordynacja rozwiązań awaryjnych z polityką bezpieczeństwa | X | X | X |
| Koordynacja rozwiązania awaryjnego z zabezpieczeniami systemu | X | X | X |
| Rozważenie gorących zapasowych miejsc pracy i umów wzajemnych | X | | X |
| Koordynacja z dostawcami | | X | X |
| Wdrożenie umów SLA z dostawcami | X | X | X |
| Określenie wskazówek dotyczących zapisywania danych na komputerach osobistych | X | | |
| Standaryzacja sprzętu i oprogramowania | X | | |
| Przechowywanie zapasowych kopii danych poza miejscem ich przetwarzania | X | X | X |
| Przechowywanie kopii oprogramowania poza miejscem jego instalowania | X | X | X |

| Czynniki brane pod uwagę w zakresie rozwiązań awaryjne | Systemy klient/serwer | Systemy telekomunikacyjne | Systemy klasy mainframe |
|---|---|---|---|
| **Rozwiązania awaryjne** | | | |
| Tworzenie kopii zapasowych systemu, aplikacji i/lub danych | X | X | X |
| Zapewnienie interoperacyjności między komponentami | X | | |
| Identyfikacja pojedynczych punktów awarii | | X | |
| Obrazy dysków | X | | |
| Wdrożenie rozwiązań pozwalających na tolerowanie błędów | | | X |
| Wdrożenie rozwiązań równoważących obciążenie | X | | X |
| Zastosowanie redundancji w krytycznych miejscach systemu | X | X | X |
| Wdrożenie rozwiązań z zakresu przechowywania danych | | | X |
| Integracja zdalnego dostępu i łączności bezprzewodowej | X | X | |
| Replikacja danych | X | | X |
| Stosowanie zasilania bezprzerwowego | X | | X |

# ZAŁĄCZNIK A - PRZYKŁADOWE SZABLONY PLANU AWARYJNEGO SYSTEMU INFORMATYCZNEGO

## ZAŁĄCZNIK A1 – PRZYKŁADOWY SZABLON DLA SYSTEMÓW O NISKIM WPŁYWIE INCYDENTU

(dokument w odrębnym pliku)

## ZAŁĄCZNIK A2 – PRZYKŁADOWY SZABLON DLA SYSTEMÓW O UMIARKOWANYM WPŁYWIE INCYDENTU

(dokument w odrębnym pliku)

## ZAŁĄCZNIK A3 – PRZYKŁADOWY SZABLON DLA SYSTEMÓW O WYSOKIM WPŁYWIE INCYDENTU

(dokument w odrębnym pliku)

# ZAŁĄCZNIK B – PRZYKŁADOWA ANALIZA WPŁYWU NA BIZNES (BIA) I SZABLON BIA

(dokument w odrębnym pliku)

# ZAŁĄCZNIK C – NAJCZĘŚCIEJ ZADAWANE PYTANIA

(dokument w odrębnym pliku)

# ZAŁĄCZNIK D – ZAGADNIENIA DOTYCZĄCE ZAANGAŻOWANIA PERSONELU W PLANOWANIU AWARYJNYM

(dokument w odrębnym pliku)

# ZAŁĄCZNIK E – ZABEZPIECZENIA W PLANOWANIU AWARYJNYM

(dokument w odrębnym pliku)

# ZAŁĄCZNIK F – PLANOWANIE AWARYJNE A CYKL ŻYCIA SYSTEMU (SDLC)

(dokument w odrębnym pliku)

# ZAŁĄCZNIK G – SŁOWNIK

**PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA**

# ZAŁĄCZNIK H – AKRONIMY

**PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA**