

ZARZĄDZANIE DZIAŁEM TECHNOLOGII INFORMACYJNYCH W FIRMIE

Streszczenie

Artykuł bazuje na bibliotece ITIL® (Information Technology Infrastructure Library). Biblioteka ta dostarcza pełnego, konsekwentnego i spójnego zestawu najlepszych praktyk dla zarządzania usługami IT (IT Service Management), wprowadza wspólny słownik pojęć, systematykę procesów IT i relacji między nimi, promuje jakościowe podejście w celu osiągnięcia biznesowej efektywności oraz skutecznego użytkowania systemów teleinformatycznych. W artykule omówiono podstawy biblioteki najlepszych praktyk ITIL®. Dokonano również krótkiego opisu procesów oraz funkcji, składających się na model zarządzania usługami IT według ITIL®.

Presented article based on ITIL® (Information Technology Infrastructure Library). ITIL® provides a set of comprehensive, consistent and coherent codes of “best practices” for quality IT service management as well as introduces the key common dictionary, semantic of the IT processes and relations between each other, promotes quality approach for business effectiveness in the use of IT. This article has been designed as an introductory overview for anyone who has an interest or need to understand the objectives, content and coverage of ITIL®.

1. WPROWADZENIE DO ITIL®

ITIL® (Information Technology Infrastructure Library) to biblioteka najlepszych praktyk (best practices) dotyczących budowy i zarządzania organizacją IT. Zostały one zebrane i opracowane przez ekspertów, konsultantów, dostawców rozwiązań IT oraz użytkowników. ITIL® stanowi podstawę dla budowy organizacji procesowej, której celem jest dostarczanie usług a nie technologii. Wprowadza systematykę procesów IT, relacje między nimi, wskazuje kluczowe czynności, definiuje role, zakresy obowiązków i odpowiedzialności. W konsekwencji pozwala spojrzeć na organizację IT jak na jeden spójny mechanizm, którego celem jest podnoszenie jakości dostarczanych usług przy minimalnych kosztach. Dodatkowo ITIL® wprowadza wspólny

¹Dr inż. Waldemar Łabuda jest wykładowcą w Warszawskiej Wyższej Szkole Informatyki.

słownik pojęć i platformę komunikacyjną wewnątrz organizacji IT, a przede wszystkim na linii biznes - IT. ITIL® jest neutralny względem organizacji, technologii i dostawców. Niezależny od wielkości organizacji, używanego przez nią sprzętu i oprogramowania oraz dostawców, z którymi współpracuje. Model zarządzania usługami IT według ITIL® jest właściwy zarówno dla komercyjnej organizacji IT dostarczającej usługi dla klienta zewnętrznego, jak i dla działu IT wewnątrz firmy, który dostarcza usługi jedynie dla klienta wewnętrznego. ITIL® stanowi obecnie standard zarządzania usługami IT wspierając i uzupełniając standard ISO9001. Promuje podejście jakościowe dla osiągnięcia biznesowej efektywności oraz skutecznego użytkowania systemów teleinformatycznych. ITIL® jest ogólnie dostępny (public domain)[4].

W 1989 roku Central Computer and Telecommunication Agency (CCTA) działająca przy rządzie Wielkiej Brytanii opublikowała pierwsze składniki biblioteki ITIL®. Początkowo biblioteka ta miała stanowić wsparcie dla projektów z zakresu zarządzania w celu uporządkowania obszaru IT w instytucjach rządu brytyjskiego i zarządzanych przez niego spółkach. W roku 2000 CCTA została włączona do Office of Government Commerce (OGC), biura powołanego przy rządzie brytyjskim (OGC jest obecnie właścicielem biblioteki ITIL® i koordynuje prace rozwojowe dotyczące tego standardu). Współpracując z British Standards Institution (BSI) oraz IT Service Management Forum (itSMF), w roku 2001 OGC opublikowała pierwsze zmiany w ITIL®. Od 2004 roku rozpoczęły się prace nad standardem ITIL®3[5].

Na bibliotekę „dobrych praktyk” ITIL® składają się następujące publikacje: Service Support, Service Delivery, ICT Infrastructure Management, Application Management, Planning to Implement Service Management, Security Management, Software Asset Management oraz The Business Perspectives. Dla osób rozpoczynających swoją przygodę z ITIL® godne polecenia są publikacje [1] i [2] oraz szkolenie [4].

Przykładowymi i wydaje się, że najbardziej znanymi narzędziami bazującymi na filozofii ITIL® są:

- Remedy IT Service Management (Remedy IT Service Management suite 5.5),
- Peregrine ServiceCenter (ServiceCenter 6.1),
- HP OpenView Service Desk (OpenView Service Desk 4.5),
- CA Unicenter Service Desk (Unicenter ServicePlus Service Desk 6.0).

Wszystkie wymienione wyżej narzędzia wspierają następujące procesy: Zarządzanie Incydemem, Zarządzanie Problemem, Zarządzanie Zmianą, Zarządzanie Konfiguracją, Zarządzanie Dostępnością, Zarządzanie Wersją oraz Zarządzanie Poziomem Usług [5].

Podstawowymi modelami opartymi na bibliotece „dobrych praktyk” ITIL® są:

- Microsoft Operations Framework (MOF),

- HP IT Service Management Reference Model,
- SunTone Initiative,
- IPW Model (KPN Telecom and Quint Wellington Redwood).

Model MOF jest adaptacją filozofii ITIL® dopasowaną do potrzeb organizacji korzystających z technologii Microsoft. Stanowi jedynie jej uzupełnienie, pomagając Klientom lepiej operować systemami bazującymi na technologiach Microsoft. Model został stworzony w 1999 roku, a w 2002 poddany aktualizacji. Przeznaczony jest do zarządzania etapem wsparcia operacyjnego systemów informatycznych. Zarządzanie bazuje tutaj zarówno na procesach, jak i na technologii. Podstawowym celem stosowania modelu MOF jest zmniejszenie liczby nieplanowanych przestołów systemu powstałych na skutek awarii technicznych oraz błędów procesów i człowieka. MOF składa się z trzech części: Modelu Procesu, Modelu Zespołu i Modelu Ryzyka [5].

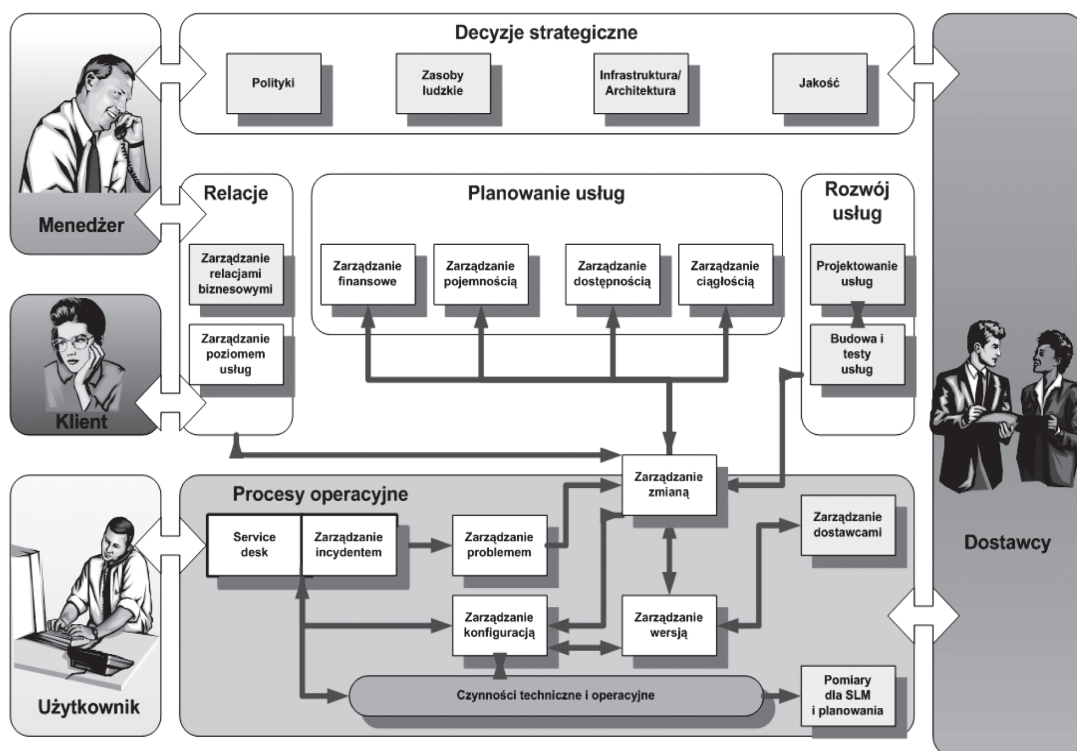
Z kolei model HP stanowi uszczegółowienie i rozszerzenie ITIL® głównie w obszarze uzgodnienia potrzeb biznesu z ofertą usług działu IT. W 1997 roku dla zaspokojenia wewnętrznych potrzeb firmy HP powstała pierwsza wersja tego modelu. Kolejna, druga wersja, z czerwca 1998 roku zawierała „HP ITSM Process Guides”, a w 2000 roku do modelu HP wprowadzony został proces Zarządzania Bezpieczeństwem (Security Management). Obecna wersja oferowana od 2003 roku pod pełną nazwą HP ITSM Reference Model 3.0 uwzględnia elementy ITIL® 2.0 oraz aktualizację o „HP Best Practices”. Składa się z pięciu podstawowych grup procesów: Service delivery assurance, Service design and management, Service development and deployment, Service Operations oraz Business-IT alignment. Celem prac nad modelem HP było stworzenie mechanizmów umożliwiających zarządzanie działem IT jak biznesem poprzez kontrolę kosztów, jakości i ryzyka, zachowując przy tym zdolność do dokonywania szybkich zmian [5].

Model zarządzania usługami IT według ITIL® składa się z dwóch obszarów tj. Service Support, Service Delivery. W obszarze Service Support wydzielono funkcję Service Desk oraz procesy: Zarządzanie Incydem (Incident Management), Zarządzanie Problemem (Problem Management), Zarządzanie Konfiguracją (Configuration Management), Zarządzanie Zmianą (Change Management), Zarządzanie Wersją (Release Management). W obszarze Service Delivery wydzielono następujące procesy: Zarządzanie Poziomem Usług (Service Level Management), Zarządzanie Dostępnością Usług (Availability Management), Zarządzanie Pojemnością (Capacity Management), Zarządzanie Finansowe dla Usług IT (Financial Management for IT), Zarządzanie Ciągłością Usług (Continuity Management) oraz Zarządzanie Bezpieczeństwem (Security Management).

Ogólny obraz modelu zarządzania usługami IT według ITIL® przedstawiono na rysunku 1[3].

Wdrożenie biblioteki dobrych praktyk w pierwszej kolejności wpływa na wzrost efektywności. Wzrost ten osiągnąć jest poprzez stosowanie gotowych i sprawdzonych propozycji oraz uproszczenie wyboru narzędzi. Ułatwione staje się również wdrożenie nowych pracowników. Biblioteka dobrych praktyk ITIL® zawiera słownik pojęć, który usprawnia komunikację pomiędzy Klientem i użytkownikiem a dostawcą usług, jak również pomiędzy IT a biznesem. Wszystko to umożliwia skupienie uwagi na zaspokojeniu potrzeb Klienta co jest korzystne dla biznesu.

Model zarządzania usługami IT według ITIL



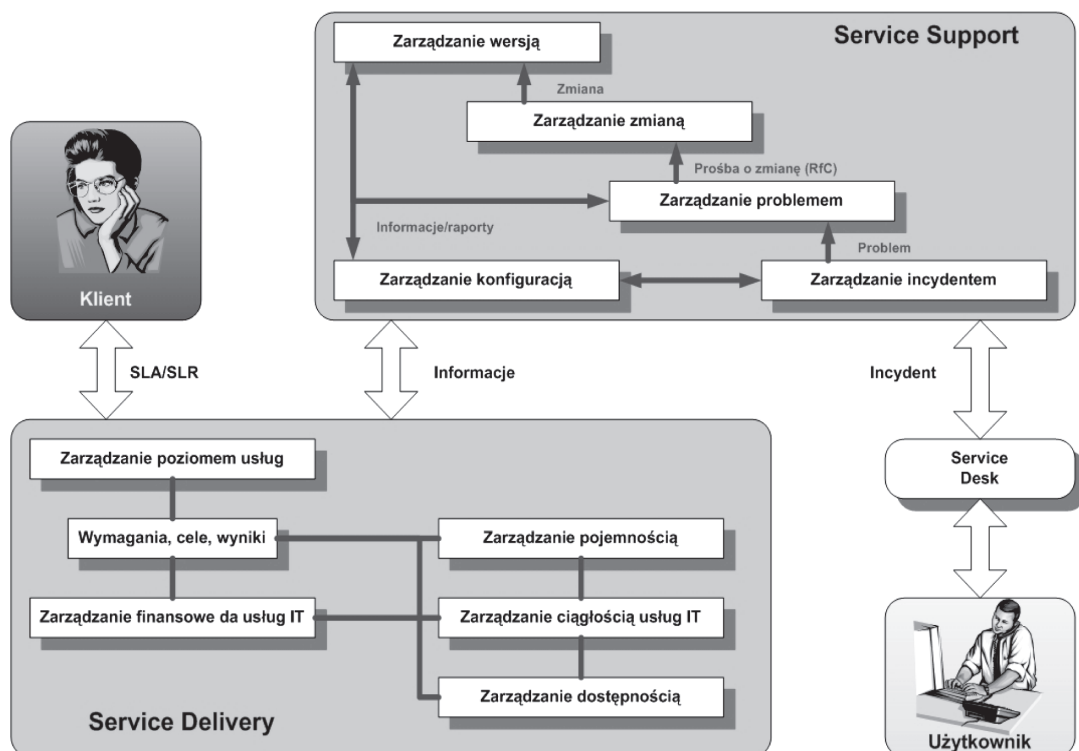
Rys. 1. Ogólny obraz modelu zarządzania usługami IT według ITIL® [3].

2. ZARZĄDZANIE USŁUGAMI IT WEDŁUG ITIL®

W niniejszym rozdziale przedstawiono elementy składowe modelu zarządzania usługami IT według ITIL®. Omówiono zatem kolejno: procesy Zarządzania Poziomem Usług i Zarządzania Konfiguracją, funkcję Service Desk, procesy Zarządzania Incydentem, Zarządzania Problemem, Zarządzania Zmianą, Zarządzania Wersją, Za-

zarządzania Finansowego dla Usług IT, Zarządzania Dostępnością, Zarządzania Pojemnością, Zarządzania Ciągłością Usług IT oraz Zarządzania Bezpieczeństwem [1][2].

Kolejność omawianych elementów składowych modelu zarządzania usługami IT według ITIL® oparta została na [4]. W tym celu model zarządzania usługami IT według ITIL® został zmieniony i przedstawiony na rysunku 2.



Rys. 2. Podstawowe elementy modelu ITIL® [4].

2.1. Zarządzanie Poziomem Usług (Service Level Management – SLM)

Co to jest usługa? Otóż usługa to jeden lub wiele systemów informatycznych wspierających proces biznesowy. Usługa może być również pojmowana jako kompletny produkt, zbiór logicznie powiązanych funkcjonalności, które w oczach Klienta stanowią całość i dostarczają wartość dodaną [4].

Celem procesu Zarządzania Poziomem Usług jest utrzymanie jakości usług IT zdefiniowanych w umowach SLA poprzez stały cykl uzgadniania, monitorowania, raportowania i przeglądu ich parametrów, jak również poprzez inicjowanie działań dla likwidacji nieakceptowanego poziomu jakości dostarczanych usług. Proces za-

wiera zatem definiowanie, monitorowanie i sterowanie poziomem dostarczanych usług oraz komunikację pomiędzy Klientem usługi IT (tym, który płaci za usługę) a jej dostawcą. Definiuje więc zadania zarówno dla dostawcy, jak i odbiorcy. Jego skutecznie wdrożenie powoduje, że dostawca odpowiada wobec odbiorcy za zdefiniowane usługi, zaś odbiorca jest odpowiedzialny za zdefiniowanie poziomów usług. Składa się z następujących aktywności [1][2]:

- negocjowanie i definiowanie, a następnie mierzenie i raportowanie parametrów usług,
- stałe podnoszenie poziomu usług zgodnie z planem SIP (Service Improvement Programme),
- przeglądanie umów SLA, OLA i UIC,
- utrzymywanie katalogu usług.

W ramach procesu Zarządzania Poziomem Usług powstaje katalog usług. Stawia on listę usług oferowanych przez organizację IT. Opis każdej usługi w katalogu może zawierać: charakterystykę usługi, Klienta i użytkowników, właściciela usługi, parametry umowy SLA, listę umów OLA oraz kontraktów UIC. Procesem SLM zarządza Service Level Manager. Odpowiada on od strony dostawcy za realizację wszystkich aktywności znajdujących się w zakresie procesu. Koordynuje usługi dostarczane przez dostawców wewnętrznych (umowy OLA), których suma działań składa się na realizację umowy SLA dla Klienta. W procesie tym definiowane są następujące rodzaje umów [4]:

- SLA (Service Level Agreement). Definiuje parametry usług pomiędzy Klientem i dostawcą usług IT,
- OLA (Operational Level Agreement). Definiuje parametry usług wewnętrznych dostarczanych przez jednostki operacyjne organizacji IT,
- UIC (Underpinnig IT Contracts). Opisuje zobowiązania zewnętrznych dostawców usług IT.

Do korzyści wynikających z zastosowania procesu Zarządzanie Poziomem Usług można zaliczyć:

- poprawę komunikacji i wyeliminowanie nieporozumień pomiędzy Klientem a dostawcą usług IT,
- możliwość podjęcia szybkich działań naprawczych w przypadku identyfikacji słabych obszarów (monitorowanie i przeglądy usług),
- możliwość użycia umowy SLA jako podstawy do pobierania opłat za dostarczane usługi,
- zarządzanie dostawcami usług oraz lepsze dopasowanie umów OLA i kontraktów wsparcia UIC do wymaganych przez Klienta usług.

2.2. Zarządzanie Konfiguracją (Configuration Management)

Celem procesu Zarządzania Konfiguracją jest identyfikacja, zliczanie i kontrola wszystkich zasobów, dostarczenie dokładnych informacji niezbędnych dla wsparcia innych procesów Zarządzania Usługami IT, weryfikacja zapisów dotyczących konfiguracji ze stanem faktycznym, jak również usuwanie ewentualnych niezgodności. Proces ten dostarcza modelu logicznego infrastruktury IT. Kluczowymi pojęciami tutaj są [4]:

- element konfiguracji (CI – Configuration Item) to składnik infrastruktury lub obiekt powiązany z infrastrukturą, który jest (lub ma być) kontrolowany przez proces Zarządzania Konfiguracją,
- Baza Danych Zarządzania Konfiguracją (CMDB – Configuration Management DataBase) jest to repozytorium informacji o elementach konfiguracji (oprócz szczegółów dotyczących elementów konfiguracji zawiera wzajemne powiązania pomiędzy nimi),
- konfiguracja podstawowa (Configuration Baseline) jest to konfiguracja produktu lub systemu określona w konkretnym momencie w czasie (obejmuje zarówno strukturę, jak i szczegóły produktu lub systemu).

Na proces Zarządzania Konfiguracją składają się następujące aktywności [1][2]:

- planowanie i definiowanie organizacyjnych i technicznych aspektów procesu,
- identyfikowanie, selekcja i oznakowanie wszystkich elementów konfiguracji (CI) zgodnie z przyjętym poziomem szczegółowości, zdefiniowanym i dopasowanym do aktualnych potrzeb biznesowych,
- kontrola, której celem jest rejestracja w bazie CMDB jedynie zidentyfikowanych i autoryzowanych elementów konfiguracji,
- raportowanie statusu, którego celem jest rejestrowanie wszystkich (bieżących i historycznych) danych dotyczących każdego elementu konfiguracji w jego cyklu życia i śledzenia ich zmian,
- weryfikowanie istnienia elementów konfiguracji oraz sprawdzanie poprawności i aktualności zarejestrowanych w bazie CMDB danych o nich.

Kluczową rolę w procesie Zarządzania Konfiguracją pełni Configuration Manager. Jest on odpowiedzialny za politykę, standardy, procedury, planowanie w procesie oraz aktualność zapisów w bazie (CMDB). Nie oznacza to jednak, że Configuration Manager jest administratorem bazy danych CMDB.

Do korzyści wynikających z zastosowania procesu Zarządzania Konfiguracją można zaliczyć:

- dostarczanie dokładnych informacji na temat elementów konfiguracji i ich dokumentacji, co jest niezbędne dla wsparcia pozostałych procesów Zarządzania Usługami IT,

- pomoc w planowaniu finansowym poprzez identyfikację wszystkich zasobów i powiązań pomiędzy nimi,
- wizualizacja zmian w oprogramowaniu i konfiguracji sprzętu,
- poprawa bezpieczeństwa poprzez kontrolowanie wersji elementów konfiguracji będących w użyciu (w produkcji) oraz zmniejszenie (lub wyeliminowanie) liczby nieautoryzowanych aplikacji.

2.3. Funkcja Service Desk

Service Desk jest jedyną funkcją w modelu ITIL®. Service Desk to jeden punkt kontaktu (SPOC - Single Point of Contact) pomiędzy użytkownikiem usług IT a organizacją dostarczającą usługi. Jego podstawowym zadaniem jest obsługa incydentów i zapytań użytkowników. Dostarcza również interfejsy dla innych procesów zarządzania usługami IT zgodnie z ITIL®. Stanowiąc główny, operacyjny interfejs między biznesem i IT, odgrywa decydującą rolę w efektywnym zarządzaniu usługami IT. Service Desk jest odpowiedzialny za [1][2]:

- przyjmowanie i rejestrację wszystkich zgłoszeń od użytkowników i rozwiązywanie prostych incydentów, zapytań i skarg,
- wstępne rozpoznawanie wszystkich zgłaszanych incydentów, zbieranie niezbędnych informacji na ich temat, podejmowanie pierwszej próby ich rozwiązania lub przekazywanie zgłaszanych incydentów do właściwej grupy wsparcia (zgodnie z ustaloną procedurą),
- śledzenie postępów prac nad rozwiązywaniem incydentów, jak również eskalacja zgodnie z ustalonymi poziomami świadczenia usług,
- informowanie użytkowników o statusie zgłoszenia oraz przygotowywanie raportów dla kierownictwa IT.

Kluczowe role w Service Desku zależą od wewnętrznych umów obowiązujących w organizacji IT oraz przyjętego modelu jego funkcjonowania (lokalny, centralny, wirtualny) [4].

Do korzyści wynikających z zastosowania funkcji Service Desk można zaliczyć:

- poprawę jakości dostarczanych usług IT, a w konsekwencji poprawę satysfakcji użytkowników (satysfakcja z usług IT jest silnie związana z oceną pracy Service Desku),
- wzrost dostępności usług poprzez wskazanie użytkownikom jednego punktu kontaktu (koniec z traktowaniem użytkownika, jak petenta),
- profesjonalną obsługę i szybsze rozwiązywanie zgłoszeń użytkowników (według ITIL® do 80% zgłoszeń incydentów powinien rozwiązać Service Desk),
- lepsze zarządzanie i kontrolowanie infrastruktury teleinformatycznej oraz bardziej efektywne wykorzystanie zasobów wsparcia (ludzi, sprzętu, oprogramowania),

- lepsze zarządzanie informacją, a więc podejmowanie właściwych decyzji dotyczących wsparcia.

2.4. Zarządzanie Incydem (Incident Management)

Przed omówieniem procesu Zarządzania Incydem należy wprowadzić kilka podstawowych pojęć. Oto one [4]:

- incydent to każde zdarzenie, które nie jest częścią standardowego działania usługi, i które powoduje (lub może powodować) przerwę w dostarczaniu usługi lub obniżenie jej jakości. Przyczyną incydemu może być uszkodzenie elementu infrastruktury IT, np.: przerwa w działaniu poczty elektronicznej lub spadek wydajności tej usługi poniżej poziomu zagwarantowanego w umowie, spowodowany awarią serwera pocztowego,
- prośba o usługę (Service Request) to zdarzenie, którego przyczyną nie jest uszkodzenie infrastruktury IT. Prośbą o usługę może być np.: prośba o zainstalowanie nowej wersji oprogramowania, czy prośba o zwiększenie dostępnej przestrzeni na dysku sieciowym. W praktyce sposób postępowania ze zgłoszeniami spowodowanymi uszkodzeniami w infrastrukturze IT oraz prośbami o usługę jest podobny,
- problem to nieznaną przyczyną jednego lub wielu incydentów,
- znany błąd to incydent lub problem, którego przyczyną jest znana, i dla którego została zidentyfikowana tymczasowa droga postępowania (work-around) lub trwała alternatywa,
- prośba o zmianę (RfC) to forma używana do zapisu szczegółów dotyczących żądania zmiany dowolnego elementu konfiguracji, procedury lub innego elementu związanego z tą infrastrukturą.

Zadaniem procesu Zarządzania Incydem jest przywrócenie normalnego działania usługi w jak najkrótszym czasie, przy zapewnieniu minimalnego wpływu na biznes, możliwie najwyższego poziomu dostępności oraz utrzymania gwarantowanego poziomu usługi. W skład procesu wchodzi następujące aktywności: wykrywanie i rejestrowanie incydentów, śledzenie, ich klasyfikacja i próba rozwiązania, badanie i diagnoza, rozwiązywanie incydentów w oparciu o bazę wiedzy i przywrócenie normalnego działania usługi, zamykanie incydentów [1][2].

Kluczową rolę w procesie Zarządzania Incydem odgrywa Service Desk, rejestrując i śledząc postępy prac nad rozwiązaniem incydemu. Dlatego też stanowisko Service Desk Managera oraz rola właściciela procesu Zarządzania Incydem (Incident Managera) jest często łączona.

Przy rozwiązywaniu incydentów kierujemy się priorytetem. Priorytet, wyznaczany w celu zaalokowania zasobów IT niezbędnych do rozwiązania incydemu, jest kombinacją wpływu na infrastrukturę IT i pilności jego rozwiązania.

Do korzyści wynikających z zastosowania procesu Zarządzania Incydem można zaliczyć:

- minimalizowanie niekorzystnego wpływu incydentów na biznes, poprzez ich szybkie rozwiązywanie, jak również wyeliminowanie incydentów nigdzie nie zarejestrowanych i nierozwiązanych,
- poprawę jakości usługi, śledzenie wyników w odniesieniu do gwarancji zapisanych w umowach SLA,
- poprawę wykorzystania personelu IT, a tym samym wzrost efektywności dostarczania usług,
- aktualizację i doprecyzowanie informacji o elementach konfiguracji w bazie CMDB poprzez ciągłą weryfikację prowadzoną podczas rejestracji kolejnych incydentów.

2.5. Zarządzanie Problemem (Problem Management)

Proces Zarządzanie Problemem koncentruje się na wykrywaniu przyczyn powiązanych ze sobą incydentów oraz tworzeniu rozwiązań zmierzających do uniknięcia wszelkich przyszłych incydentów tego samego typu. Zatem Zarządzanie Problemem jest procesem odpowiadającym za znalezienie przyczyny incydentu, jak również sposobu na przywrócenie poprawnego działania usługi IT. Poza tym Zarządzanie Problemem zajmuje się poszukiwaniem nowych rozwiązań dla nowych, niestandardowych zgłoszeń. Kluczowymi pojęciami obecnymi w procesie Zarządzania Problemem są [4]:

- kontrola problemu, która polega na przekształcaniu problemów w znane błędy (Known Error),
- kontrola błędów polegająca na rozwiązywaniu znanych błędów w procesie Zarządzania Zmianą.

W zakresie procesu Zarządzania Problemem znajdują się następujące aktywności [1][2]:

- zapewnianie szybkiego i efektywnego rozwiązywania problemów zgodnie z potrzebami biznesowymi,
- identyfikowanie i rozwiązywanie problemów oraz znanych błędów, a tym samym minimalizowanie możliwości ich wystąpienia w przyszłości,
- zwiększanie produktywności personelu wspierającego oraz dostarczanie odpowiedniej informacji zarządczej.

Proces Zarządzania Problemem nadzoruje Problem Manager. Jest on odpowiedzialny za efektywne funkcjonowanie procesu oraz nadzór nad rozwiązywaniem problemów.

Do korzyści wynikających z zastosowania procesu Zarządzania Problemem można zaliczyć:

- poprawę jakości usług IT,
- zmniejszenie liczby incydentów (w pierwszej kolejności tych o dużym wpływie na biznes oraz systematycznie powtarzających się),
- inicjowanie systemowych rozwiązań eliminujących ponowne pojawianie się incydentów danego typu,
- zasilanie Bazy wiedzy informacjami o problemach, znanych błędach i ich rozwiązaniach,
- poprawa wskaźników rozwiązywalności zgłoszeń przez Service Desk.

2.6. Zarządzanie Zmianą (Change Management)

Zmiana to proces przejścia z jednego, zdefiniowanego stanu do drugiego. Zmianą może być dodanie, zmodyfikowanie lub usunięcie zatwierdzonego, wspieranego lub podstawowego elementu konfiguracji, a więc: elementu sieci, oprogramowania, aplikacji, środowiska, systemu, urządzenia przenośnego lub związanej z nim dokumentacji [4].

Proces Zarządzanie Zmianą zapewnia, że dla wszystkich zmian przyjęte zostały i są używane standardowe metody, procesy i procedury niezbędne dla zapewnienia skuteczności i efektywności wprowadzania zmian. Zapewnia więc biznesową równowagę pomiędzy potrzebą zmiany i ryzykiem negatywnego wpływu zmiany na usługi IT. Proces Zarządzania Zmianą zawiera następujące aktywności [1][2]:

- inicjowanie zmian i rejestrowanie wniosków o zmianę (RfC - Request for Change), przy czym RfC używa się do zapisu szczegółów dotyczących zmiany dowolnego elementu konfiguracji, procedury lub innego elementu związanej z infrastrukturą,
- oszacowanie wpływu, kosztu, korzyści i ryzyka proponowanych zmian,
- zarządzanie i koordynację budowy, testów i implementacji zmian oraz monitorowanie i raportowanie implementacji zmiany.

Kluczową rolę w procesie Zarządzania Zmianą odgrywa Change Manager, który ustala i nadzoruje przebieg procesu. Działania Change Managera wspierane są przez Radę ds. Zmiany (CAB – Change Advisory Board) w przypadku normalnych zmian oraz Komitet Nadzwyczajny (CAB/EC - Change Advisory Board / Emergency Committee) posiadający uprawnienia do podejmowania decyzji odnośnie pilnych zmian w sytuacjach awaryjnych [4].

Wyróżnia się następujące modele zmian [4]:

- standardowa zmiana - zaakceptowane wcześniej rozwiązanie zidentyfikowanego i relatywnie prostego zestawu wymagań, np.: zakładanie profilu użytkownika, wymiana drukarki lub monitora,

- normalna zmiana – podstawowy model zmiany, realizacja zmiany przeprowadzana jest najczęściej w formie projektu (metodyka zarządzania projektami np.: PRINCE2, PMI),
- pilna zmiana – umożliwi szybkie przejście przez proces normalnej zmiany z pominięciem lub uproszczeniem niektórych etapów (np. testów), przy założonym ryzyku. Model stosowany w sytuacjach awaryjnych, gdzie czas implementacji zmiany jest krytyczny.

Do korzyści wynikających z zastosowania procesu Zarządzania Zmianą można zaliczyć:

- lepsze dopasowanie usług IT do aktualnych potrzeb biznesowych, jak również zmniejszenie niekorzystnego wpływu zmiany na inne usługi IT,
- precyzyjne oszacowanie kosztów projektowanej zmiany przed ich wprowadzeniem,
- ułatwienie Zarządzania Problemem i Dostępnością usług poprzez wykorzystanie informacji zarządczych związanych ze zmianą,
- podniesienie efektywności kluczowych pracowników IT poprzez zmniejszenie liczby problemów powstających w wyniku błędnych zmian.

2.7. Zarządzanie Wersją (Release Management)

Wersja to zbiór zatwierdzonych zmian w usłudze IT. Zarządzanie Wersją jest ściśle związane z procesami Zarządzania Konfiguracją oraz Zarządzania Zmianą. Procesy te korzystają z tych samych baz danych zawierających informacje o elementach konfiguracji (CMDB) [4].

Zarządzanie Wersją to kompleksowe spojrzenie na zmianę usługi IT oraz zapewnienie, że wszystkie aspekty wersji, zarówno techniczne (sprzęt), jak i nietechniczne (oprogramowanie) zostały łącznie rozpatrzone. Proces Zarządzania Wersją ma zastosowanie dla: dużych i krytycznych wymian sprzętu (Roll-out), wprowadzania nowych wersji oprogramowania itp. Zarządzanie Wersją obejmuje następujące aktywności [1][2]:

- planowanie i nadzorowanie pomyślnych wdrożeń nowych oraz zmienionych wersji oprogramowania, jak również związanego z tym sprzętu i dokumentacji,
- współpracę pomiędzy procesami Zarządzania Wersją, a Zarządzania Zmianą dla uzgodnienia właściwej zawartości oraz planu wdrożenia dla wersji,
- zapewnienie, że wszystkie elementy, które zostały wdrożone lub zmienione są bezpieczne i możliwe do śledzenia poprzez bazę CMDB,
- zarządzanie oczekiwaniami klientów i użytkowników dotyczącymi wersji i procesu wdrożenia.

Kluczową rolę w procesie pełni Release Manager odpowiedzialny za cały proces. Jego działania wspierane są analogicznie jak w procesie Zarządzania Zmianą przez

Radę ds. Zmiany (CAB – Change Advisory Board) oraz w sytuacjach nagłych - Komitet Nadzwyczajny (CAB/EC - Change Advisory Board / Emergency Committee).

Kluczowymi pojęciami w procesie Zarządzania Wersją są [4]:

- biblioteka stosowanego oprogramowania (DSL - Definitive Software Library) jest to miejsce przechowywania głównych kopii wszystkich kontrolowanych w organizacji wersji oprogramowania,
- magazyn stosowanego sprzętu (DHS - Definitive Hardware Store) jest to magazyn stosowanych części zamiennych sprzętu (opis części powinien znajdować się w bazie CMDB),
- testowanie i Plany Wycofań (Testing and Back-out Plans) - wersje powinny podlegać testom i akceptacji użytkowników przed ich wydaniem, natomiast Plany Wycofań są konieczne na wypadek całkowitych lub częściowych niepowodzeń we wdrożeniu wersji,
- Roll-out – to dostarczenie, instalacja i uruchomienie zintegrowanego zestawu nowych lub zmienionych elementów infrastruktury w logicznych lub fizycznych częściach organizacji.

Do korzyści wynikających z zastosowania procesu Zarządzania Wersją można zaliczyć:

- poprawę jakości usług, jako wynik wyższego wskaźnika sukcesu we wdrażaniu nowych wersji i minimalizacji zakłóceń w obszarze biznesu,
- pewność, że używany sprzęt i oprogramowanie jest znanej jakości; redukcja możliwości użycia nielegalnego, złego lub nieautoryzowanego oprogramowania,
- zwiększenie zdolności organizacji do radzenia sobie ze zbyt wysokim poziomem zmian (zmian zbyt licznych, które powodują nieuzasadnione przerwy w dostarczaniu usług),
- lepsze wykorzystanie zasobów oraz określanie wymagań dla biznesu i pracowników wsparcia usług.

2.8. Zarządzanie Finansowe dla Usług IT (Financial Management for IT)

IT Financial Management jest procesem, który dostarcza narzędzi do efektywnego zarządzania zasobami IT oraz zasobami finansowymi wykorzystanymi dla dostarczania usług IT. Zadaniem procesu jest budowa efektywnego zarządzania finansowego. W skład tego procesu wchodzi następujące aktywności [1][2]:

- Obliczanie przez organizację całkowitych wydatków związanych z usługami IT i przypisanie ich do usług dostarczanych Klientowi,
- dostarczanie precyzyjnych informacji zarządczych dotyczących zarówno bieżącej pracy IT, jak i w przypadkach inwestycji IT dotyczących zmian i usług IT,

- kontrolowanie i zarządzanie budżetem IT oraz umożliwianie jasnego i sprawiedliwego zwrotu kosztów (poprzez pobierane opłaty) za świadczone usługi IT.

Procesem zarządza Financial Manager. Jest on odpowiedzialny za zaprojektowanie modelu kosztowego, na którym będzie opierało się zarządzanie finansowe IT. Odpowiada również za budżetowanie usługi i analizę tego budżetu. Budżetowanie i rachunkowość jest podstawą w dostarczaniu i utrzymaniu efektywności kosztów i skuteczności usług. Te czynności umożliwiają organizacji [4]:

- prognozowanie nakładów niezbędnych do uruchomienia usług IT na dany okres, porównywanie przewidywanych i poniesionych nakładów oraz obliczanie rzeczywistych nakładów w badanym okresie,
- obliczanie kosztów dostarczanych usług IT,
- pobieranie opłat - pokazuje klientom konieczność wyważenia pomiędzy potrzebami i możliwościami finansowymi, a także zmusza klientów do optymalizowania korzystania z usług IT. Ta czynność umożliwia organizacji: odzyskiwanie kosztów usług IT od Klientów usług, obsługiwane usługi IT jako część biznesu (jeśli jest to konieczne), wpływanie na zachowania Klientów i Użytkowników, umożliwianie porównania z alternatywnymi dostawcami usług.

Do korzyści wynikających z zastosowania procesu Zarządzania Finansowego dla usług IT można zaliczyć:

- redukcja kosztów w dłuższym okresie,
- wspieranie decyzji o inwestycjach IT poprzez precyzyjne informacje o kosztach,
- bardziej efektywne wykorzystanie IT przez biznes,
- pewność, że biznes dostarcza dostatecznych funduszy, aby uruchomić wymagane usługi IT,
- oparcie decyzji podejmowanych w ramach IT na rzeczywistych możliwościach i potrzebach biznesu,
- upraszczanie obciążania klientów korzystających z usług, co pozwala na lepsze zarządzanie wewnętrznym budżetem IT.

2.9. Zarządzanie Dostępnością (Availability Management)

Proces Zarządzania Dostępnością zapewnia, że usługi są dostępne wtedy, kiedy Klient ich potrzebuje. Celem procesu jest optymalizowanie zdolności infrastruktury IT oraz organizacji wsparcia do dostarczania efektywnego kosztowo i stałego poziomu dostępności usług. W skład tego procesu wchodzi następujące aktywności [1][2]:

- optymalizowanie dostępności poprzez monitorowanie i raportowanie wszystkich kluczowych elementów infrastruktury IT, jak również określanie wymagań dostępności w relacjach biznesowych,

- prognozowanie i projektowanie oczekiwanych poziomów dostępności i bezpieczeństwa, opracowanie Planu Dostępności,
- zbieranie, analizowanie i utrzymywanie danych o dostępności usług IT oraz raportowanie,
- czuwanie nad tym, żeby poziomy dostarczanych usług odpowiadały poziomom dostępności usług zdefiniowanym w umowach SLA,
- systematyczne podnoszenie dostępności usług i ich komponentów.

Za właściwe zaplanowanie elementów procesu i związanych z nim metod i technik, jak również za regularny przegląd procesu i poszukiwanie usprawnień odpowiedzialny jest Availability Manager. Kluczowymi pojęciami w procesie Zarządzania Dostępnością są [4]:

- dostępność (Availability) - procent uzgodnionych godzin świadczenia usługi, w których usługa jest dostępna,
- niezawodność (Reliability) - zapobieganie awariom i zdolność zapewniania ciągłości świadczenia usług, bez przestojów,
- możliwość utrzymania (Maintainability) - zdolność do przywracania usługi do normalnego działania,
- możliwość świadczenia usług (Serviceability) - wsparcie, którego udzielają związani umowami dostawcy zewnętrzni dostarczający komponenty infrastruktury IT.

Do korzyści wynikających z zastosowania procesu Zarządzania Dostępnością można zaliczyć:

- określanie podstawowych potrzeb biznesowych dotyczących wysokiej dostępności,
- pomiar poziomu dostępności dla pełnego wsparcia Zarządzania Poziomem Usług,
- identyfikacja niedostatecznych poziomów usług i podejmowanie działań korygujących,
- redukcja częstotliwości i czasu trwania awarii IT.

2.10. Zarządzanie Pojemnością (Capacity Management)

Zarządzanie Pojemnością zapewnia, że zasoby tworzące infrastrukturę IT odpowiadają rosnącym wymaganiom biznesowym w sposób maksymalnie efektywny kosztowo i czasowo. Celem procesu jest zrozumienie wymagań biznesowych tak, aby dostarczać usługi IT realizując zobowiązania zapisane w umowach SLA i mając na uwadze oczekiwaną ich wydajność. W zakresie procesu znajdują się [1][2]:

- monitorowanie wydajności usług IT, jak również optymalizowanie działań tak, aby skutecznie wykorzystywać posiadane zasoby,
- tworzenie planu rozwoju potrzeb przewidującego niezbędne zasoby IT niezbędne dla osiągnięcia uzgodnionych poziomów usług,

- zrozumienie bieżącego zapotrzebowania na zasoby IT i na tej podstawie przewidywanie przyszłych wymagań,
- analizowanie wpływu potrzeb biznesowych na zasoby w połączeniu z innymi procesami Zarządzania Usługami IT.

Kluczowymi pojęciami w procesie Zarządzania Pojemnością są [4]:

- Zarządzanie pojemnością biznesową (Business Capacity Management - BCM) - zapewnia, że obecne i przyszłe wymagania biznesu dotyczące pojemności usług IT są brane pod uwagę, a niezbędne działania zmierzające do wdrożenia zmian są planowane i wdrażane we właściwym czasie,
- Zarządzanie pojemnością usług (Service Capacity Management - SCM) - przekłada wymagania biznesowe na określone usługi informatyczne. Zapewnia więc, że pojemność usług spełnia wymagania biznesowe, a parametry definiujące tę pojemność, zapisane w umowie SLA, są monitorowane i mierzone (dane zapisywane, analizowane i raportowane),
- Zarządzanie pojemnością zasobów (Resource Capacity Management - RCM) - skupia się na zarządzaniu składnikami infrastruktury IT i zapewnia, że wszystkie zasoby IT są monitorowane i mierzone a zbierane dane są zapisywane i raportowane.

Do korzyści wynikających z zastosowania procesu Zarządzania Pojemnością można zaliczyć:

- zwiększanie skuteczności i oszczędności wynikających z bardziej ekonomicznego dostarczania usług IT,
- opóźnianie wydatków, dla których jest to możliwe oraz eliminowanie drogich „panicznych” zakupów, a więc bardziej świadome nabywanie zasobów IT,
- redukcja ryzyka wystąpienia problemów i uszkodzeń,
- lepsze relacje z klientami i użytkownikami z większym zrozumieniem poziomów usług i SLA,
- poprawa jakości usług poprzez lepszą kontrolę.

2.11. Zarządzanie Ciągłością Usług IT (Continuity Management)

Zarządzanie Ciągłością Usług IT jest rozumiane jako wsparcie procesu ciągłości biznesu (Business Continuity Process) w całej organizacji poprzez przywrócenie świadczenia usług IT w wymaganym i uzgodnionym czasie. Skutki przerwy w dostarczaniu usług IT mogą spowodować: straty finansowe, utratę danych, niezadowolenie Klientów, niekorzystny wpływ na wizerunek organizacji IT, wzrost kosztów spowodowany koniecznością przywrócenia normalnego funkcjonowania IT i odzyskania danych itp. W zakresie procesu znajdują się [1][2]:

- opracowanie planu przywrócenia IT (części ogólnego Planu Zapewnienia Ciągłości Biznesu),

- zapewnianie funkcjonowania biznesu poprzez redukcję wpływu zagrożeń (katastrofy, porażki),
- redukowanie wrażliwości biznesu na zagrożenia przez efektywną analizę ryzyka i zarządzanie ryzykiem,
- zapobieganie utracie zaufania Klientów i użytkowników.

W procesie przewidziane są role dla osób z każdego poziomu zarządzania zarówno w sytuacji normalnego funkcjonowania biznesu, jak i w sytuacjach kryzysowych. Jednak osobą odpowiedzialną za budowę Planów ciągłości usług IT jest IT Service Continuity Plan Manager (ITSCPM).

Kluczowymi pojęciami w procesie Zarządzania Pojemnością są [4]:

- Plan Ciągłości Biznesu (Business Continuity Plan - BCP) - plan przedsiębiorstwa, utrzymania przy życiu kluczowego obszaru biznesowego (core business) oraz przywrócenia, możliwie jak najszybciej, działania pozostałych procesów biznesowych w przypadku katastrofy,
- Plan ciągłości usług IT (IT Service Continuity Plan - ITSC Plan) - plan dostawcy, wsparcia kluczowego obszaru biznesowego przedsiębiorstwa Klienta oraz przywrócenia działania usług w przypadku katastrofy,
- CRAMM (CCTA Risk Analysis Management Model) – to metoda zbierania informacji na temat ryzyka i zarządzanie nim.

Do korzyści wynikających z zastosowania procesu Zarządzania Ciągłością usług IT można zaliczyć:

- możliwość wynegocjowania mniejszych składek ubezpieczeniowych oraz dostosowanie działań do obowiązujących regulacji prawnych i innych kontrolowanych wymagań,
- poprawienie relacji między biznesem a IT (przez lepsze zrozumienie priorytetów biznesowych),
- zrozumienie ryzyka oraz zarządzanie nim,
- redukowanie przerw w biznesie podczas incydentu z możliwością przywrócenia efektywnych usług zgodnie z biznesowymi priorytetami
- zwiększanie zaufania klientów i wiarygodności oraz potencjalnie wzrost przewagi nad konkurencją.

2.12. Zarządzanie Bezpieczeństwem (Security Management)

Celem procesu jest zapewnienie bezpieczeństwa biznesu i ograniczenie szkód poprzez profilaktykę oraz minimalizowanie wpływu incydentów naruszających bezpieczeństwo. W zakresie procesu znajdują się [1][2]:

- kontrola poziomu bezpieczeństwa niezbędna dla zareagowania na zmieniające się wymagania biznesowe, architekturę elementów infrastruktury, zagrożenia (wewnętrzne i zewnętrzne),

- zarządzanie incydentami związanymi z bezpieczeństwem,
- przeprowadzanie audytów pokazujących skuteczność kontroli poziomu bezpieczeństwa i właściwość stosowanych mierników,
- raportowanie statusu bezpieczeństwa informacji.

Zarządzanie bezpieczeństwem IT powinno być elementem opisu stanowiska każdego menedżera IT [4].

3. ZASADY STOSOWANIA ITIL® [3]

Skuteczność usługowego modelu zarządzania informatyką promowanego przez ITIL® potwierdzają międzynarodowe badania i praktyka. Model procesów ITIL® daje kompleksowe spojrzenie na informatykę, porządkuje całą organizację, a nie tylko wybrane jej elementy. Wskazówki zawarte w bibliotece ITIL® wyznaczają kierunki działań dla poprawy efektywności działów IT. Zwracają uwagę na najczęściej popełniane błędy, mówią jak ich unikać, podpowiadają rozwiązania, które sprawdziły się w wielu innych organizacjach. ITIL® opisuje najlepsze praktyki w zakresie zarządzania usługami IT, na podstawie których należy opracować szczegółowe procedury i instrukcje dostosowane do specyfiki usług dostarczanych przez wdrażającą je firmę. Nie należy zatem w ITIL® szukać konkretnych procedur i instrukcji, gotowych do zastosowania w dowolnej organizacji. Stosowanie się do dobrych praktyk ITIL® to między innymi:

- redukcja kosztów - zarządzanie IT jak biznesem,
- komunikacja - wspólna koncepcja świata IT oraz struktury komunikacji,
- relacje z klientem - skupienie uwagi na korzyściach dla biznesu (patrzenie na informatykę oczami biznesu),
- zarządzanie jakością - ciągle doskonalenie organizacji.

Biblioteki ITIL® nie można wdrożyć, bo nie jest to narzędzie. Jeśli jednak zdecydujemy się przenieść go w całości, za jednym podejściem i zaadaptować na potrzeby organizacji, to polegniemy. Jest to zbyt szeroki obszar, by przedsięwzięcie to mogło zakończyć się powodzeniem. Dlatego konieczne jest podzielenie tego procesu na fazy, pamiętając przy tym o silnych relacjach między poszczególnymi obszarami. Wdrożenie jednego odizolowanego od całego modelu procesu również nie ma większego sensu.

W pierwszej kolejności należy skupić się na procesach najbliższych biznesowi, a więc Zarządzaniu Poziomem usług IT, Zarządzaniu Incydem i funkcji Service Desk. Jeżeli bowiem organizacja IT nie będzie potrafiła dogadać się z biznesem, nawet najlepsze wewnętrzne zasady nie pomogą w odniesieniu sukcesu, dobrym postępowaniu przez klienta i satysfakcji użytkowników.

Literatura

- [1] Ivor Macfarlane, Colin Rudd, IT Service Management, itSMF, 2005 r.
- [2] Jan van Bon, Mike Pieper, Annelies van der Venn, IT Service Management based on ITIL® – An Introduction, Third Edition. itSMF, 2005 r.
- [3] Michał Florys, Zbiór artykułów dotyczących IT Infrastructure Library, ITPartners S.A., 2005 r.
- [4] Materiały ze szkolenia „ITIL® – Foundation”, CTPartners S.A., 2005 r.
- [5] Materiały publikowane na stronie <http://www.ITIL@ife.pl>.

