

COBIT

i jego wykorzystanie dla zwiększania efektywności działania funkcji IT

Przestanką dla rozwoju metodyki COBIT jest przeświadczenie o rosnącym znaczeniu informacji jako kluczowego zasobu organizacji oraz roli, jaką pełni technologia w cyklu życia informacji. Metodyka COBIT ma być odpowiedzią na potrzebę osiągania korzyści biznesowych oraz sprawności operacyjnej, w tym optymalizacji kosztów usług IT, dzięki efektywnemu i innowacyjnemu wykorzystaniu technologii.

Metodyka COBIT kładzie duży nacisk na kwestie utrzymania ryzyka związanego z IT na akceptowalnym poziomie, przy równoczesnym zapewnieniu zgodności z obowiązującymi przepisami, regulacjami, zobowiązaniami umownymi oraz politykami. Osią przewodnią COBIT jest kaskada celów: od potrzeb interesariuszy poprzez cele organizacji, cele związane z IT, aż po poziom definiowanych metodyką czynników umożliwiających. Koncepcja czynników umożliwiających ma na celu skonkretyzowanie działań związanych z nadzorem nad technologiami informatycznymi w organizacji i zarządzania nimi tak, aby były one skuteczne i wpisywały się w zdefiniowane cele wyższego rzędu.

Obiektywna ocena dojrzałości procesów

Dzięki COBIT możliwe jest przeprowadzenie obiektywnej oceny dojrzałości procesów IT każdej organizacji bez względu na jej specyfikę i branżę. Ramy metodyki definiują 37 procesów IT przypisanych do pięciu domen obejmujących kompletny katalog działań związanych z nadzorem i zarządzaniem technologiami informatycznymi w przedsiębiorstwie, w tym procesy zarządzania IT w zakresie dopasowania, planowania i organizacji (APO), budowania, nabywania i wdrażania technologii IT (BAI), a także dostarczania, obsługi i wsparcia tych technologii (DSS) oraz procesy monitorowania i oceny (MEA).

Wykorzystanie modelu potencjału procesu opartego na normie ISO/IEC 15504 Software Engineering pozwala na skategoryzowanie każdego z procesów organizacji na poziomie od 0 – proces niekompletny do 5 – proces optymalizujący oraz skuteczną identyfikację obszarów wymagających usprawnień. Dla ułatwienia kategoryzacji każdy proces opisany jest zestawem pytań, określających podprocesy, które powinny zostać zdefiniowane, by móc zakwalifikować dany proces na odpowiedni poziom dojrzałości.

Należy podkreślić, że w przyjętym schemacie oceny już osiągnięcie poziomu 1 stanowi ważny sukces dla organizacji. Jest to o tyle istotne, że pułapką przyjętego podejścia może być chęć firmy do osiągnięcia możliwie wysokiego poziomu dojrzałości, podczas gdy każdy podmiot powinien wybrać pożądaną poziom na bazie rachunku kosztów i korzyści takiego działania oraz analizy jego wykonalności, a doświadczenie wskazuje, że bardzo rzadko uzasadnione jest celowanie w poziom najwyższe.



SIEDEM KATEGORII CZYNNIKÓW UMOŻLIWIAJĄCYCH

- **Zasady, polityki i metodyki** stanowią środek umożliwiający przełożenie pożądanego wzorca zachowań na praktyczne wytyczne dotyczące codziennego zarządzania.
- **Procesy** opisują uporządkowany zbiór praktyk i działań pozwalających na osiągnięcie określonych celów i uzyskanie zbioru wyników ułatwiających realizację ogólnych celów związanych z IT.
- **Struktury organizacyjne** to kluczowe jednostki odpowiedzialne za podejmowanie decyzji w przedsiębiorstwie.
- **Kultura, etyka i zachowanie** odnoszą się do osób oraz firm i są często niedocenianym czynnikiem sukcesu działań związanych z nadzorem i zarządzaniem.
- **Informacja** dotyczy całego przedsiębiorstwa i obejmuje wszystkie informacje wytwarzane i wykorzystywane przez firmę. Informacje są wymagane do zapewnienia właściwego funkcjonowania organizacji oraz nadzoru nad jej działalnością, ale na poziomie operacyjnym informacje są bardzo często kluczowym produktem przedsiębiorstwa.
- **Usługi, infrastruktura i aplikacje** obejmują infrastrukturę, technologię i aplikacje zapewniające firmie możliwości przetwarzania oraz usługi IT.
- **Ludzie, umiejętności i kompetencje** to czynnik dotyczący osób i jest wymagany do skutecznej realizacji wszystkich działań oraz podejmowania właściwych decyzji i przeprowadzania działań naprawczych.

Źródło: ISACA

W praktyce wykorzystanie standardu COBIT jako składowej audytu informatycznego odsuwa z głównej osi widzenia aspekty oceny technologii i infrastruktury na korzyść oceny obszaru IT w kontekście celów biznesowych organizacji oraz zapewnienia informacji o odpowiedniej jakości i użyteczności dla zastosowań biznesowych. COBIT kładzie akcenty na kwestie związane z integralnością danych, efektywnością działania organizacji oraz zapewnienia mechanizmy kontroli wewnętrznej, niezbędne



POZIOMY POTENCJAŁU COBIT, KTÓRE MOŻE OSIĄGNĄĆ PROCES:

- **Proces niekompletny** – proces nie został wdrożony lub jego cel nie został osiągnięty. Na tym poziomie nie istnieją dowody systematycznej realizacji celu procesu lub ich liczba jest znikoma.
- **Proces wykonywany (jeden atrybut)** – cel wdrożonego procesu osiągnięto.
- **Proces zarządzany (dwa atrybuty)** – opisany wyżej proces wykonywany został wdrożony w sposób zarządzany (zapewniono planowanie, monitorowanie i dostosowanie), a jego produkty działań są właściwie określone, kontrolowane i utrzymywane.
- **Proces ustanowiony (dwa atrybuty)** – opisany wcześniej proces zarządzany jest wdrażany za pomocą zdefiniowanego procesu umożliwiającego osiągnięcie wyniku procesu.
- **Proces przewidywalny (dwa atrybuty)** – opisany wcześniej proces ustanowiony działa teraz w ramach zdefiniowanych limitów w celu osiągnięcia wyników procesu.
- **Proces optymalizujący (dwa atrybuty)** – opisany wcześniej proces przewidywalny jest nieustannie doskonalony w celu realizacji istotnych aktualnych i projektowanych celów biznesowych.

Źródło: ISACA

do dostarczenia wiarygodnych informacji o osiągnięciu celów operacyjnych i kontrolnych.

Tworzenie wiarygodnych rekomendacji dotyczących rozwoju architektury IT

Dzięki dekompozycji celów interesariuszy i organizacji na cele IT oraz zobiektywizowaniu procesu oceny dojrzałości procesów IT możliwe jest tworzenie wiarygodnych rekomendacji w obszarze rozwoju docelowej architektury środowiska IT w firmie, jak również modelu funkcjonowania organizacji IT. Realizacja tak zdefiniowanych inicjatyw rozwojowych znajduje jednoznaczne odzwierciedlenie i uargumentowanie w kontekście wytycznych metodyki COBIT. Co istotne, zakres inicjatyw i ich charakter bazuje na przesłance

Nawet jeśli dzisiaj ITIL stanowi kompleksowe podejście do zarządzania usługami obejmujące obszary strategii usług oraz ustawicznego doskonalenia procesów, to **COBIT lepiej wyraża ideę ładu korporacyjnego IT jako zasad i norm niezbędnych do realizacji skutecznego nadzoru właścicielskiego, założonych celów strategicznych organizacji oraz zapewnienia zgodności z obowiązującymi w firmie regulacjami.** Prowadzi to do konkluzji, że dobrym pomysłem na zaadresowanie potrzeb biznesowych z wykorzystaniem IT może być połączenie wytycznych COBIT i ITIL.

uzyskania optymalnej wartości z IT, przy założeniu zachowania niezbędnej równowagi między osiąganiem zamierzonych korzyści a optymalizacją poziomu ryzyka i wykorzystania zasobów.

Fakt, że COBIT – w przeciwieństwie do biblioteki ITIL – jest postrzegany jako mniej praktyczny, wskazuje tylko na zasadność dalszych działań na rzecz jego upowszechnienia. Takie przekonanie może mieć podstawy w utartym postrzeganiu COBIT jako ram dostarczających odpowiedzi na pytanie „dlaczego”, podczas gdy ITIL odpowiada na pytanie „jak”, co rzekomo miałyby wskazywać na bardziej praktyczny wydźwięk zaleceń ITIL. Należy podkreślić, że w dalszym ciągu przekonanie o zasadności adaptacji standardów w obszarze ładu korporacyjnego IT utożsamiane jest bowiem z obszarem eksploatacji usług IT, w którym zdecydowanie bardziej zakorzeniony jest ITIL.

Nawet jeśli dzisiaj ITIL stanowi kompleksowe podejście do zarządzania usługami obejmujące obszary strategii usług oraz ustawicznego doskonalenia procesów, to COBIT lepiej wyraża ideę ładu korporacyjnego IT jako zasad i norm niezbędnych do realizacji skutecznego nadzoru właścicielskiego, założonych celów strategicznych organizacji oraz zapewnienia zgodności z obowiązującymi w firmie regulacjami. Taki stan rzeczy prowadzi do konkluzji, że dobrym pomysłem na zaadresowanie potrzeb

Osią przewodnią COBIT jest kaskada celów: od potrzeb interesariuszy poprzez cele organizacji, cele związane z IT, aż po poziom definiowanych metodyką czynników umożliwiających. Koncepcja czynników umożliwiających ma na celu skonkretyzowanie działań związanych z nadzorem nad technologiami informatycznymi w organizacji i zarządzania nimi tak, aby były one skuteczne i wpisywały się w zdefiniowane cele wyższego rzędu.

biznesowych z wykorzystaniem IT może być połączenie wytycznych COBIT i ITIL. Zwłaszcza że jednym z podstawowych założeń COBIT 5 jest jego wykorzystanie jako nadrzędnego integratora ram ładu i zarządzania oraz otwartość na dopasowanie do standardów i innych ram stosowanych przez organizacje w obszarach ładu organizacyjnego i technologii informatycznych.

Jak w przypadku każdego z istniejących na rynku standardów, należy pamiętać o konieczności ich dostosowania do indywidualnych potrzeb i skutecznym podejściu do ich zaaplikowania w firmie. COBIT niesie konkretne ryzyka. O jednym z nich – nadmiernej chęci pięć się po szczeblach poziomów dojrzałości – wspomniano już wcześniej. W publikacjach wspomina się również o zjawisku wyuczzonej bezradności, która może uniemożliwić przejście organizacji na kolejne wyższe poziomy dojrzałości. O ile bowiem COBIT sprawdza się na etapie przejścia przez pierwsze poziomy, o tyle w przypadku kolejnych szczebli zakorzenione w tożsamości organizacji procesy zamiast stać się przyczynkiem do dalszym zmian, mogą wywoływać efekt zgoła odmienny. Nie da się również ukryć, że COBIT stanowi ramy ambitne i obszerne, wymagające dużego doświadczenia i wiedzy na etapie ich wdrożenia. Nie zmienia to faktu, że to właśnie kompleksowość stanowi o sile metodyki, która zawiera przykłady i wzorce, a także model 7 faz cyklu życia wdrożenia ułatwiający sprostanie typowym wyzwaniom w implementacji COBIT.

*Michał Wiatr,
prezes zarządu firmy Softtutor Consulting; Softtutor Consulting realizuje usługi w zakresie audytu IT z wykorzystaniem metodyki COBIT.*



ZALETY I WADY COBIT

ZALETY

- Podejmowanie decyzji na poziomie kierowniczym jest bardziej skuteczne, gdyż COBIT pomaga w określeniu strategicznego planu IT poprzez zastosowanie kaskady celów interesariuszy na cele organizacji, cele IT oraz cele czynników umożliwiających.
- COBIT zwraca uwagę na aspekt racjonalizacji nakładów i środków na etapie tworzenia wartości dla interesariuszy, wskazując na zasadność zachowania równowagi między realizacją korzyści, optymalizacją ryzyka i wykorzystaniem zasobów.
- COBIT zapewnia model referencyjny procesu, obejmujący kompletny katalog działań związanych z nadzorem i zarządzaniem technologiami informatycznymi w organizacji, który wraz z modelem potencjału procesu opartego na normie ISO/IEC 15504 pozwala na zobiektywizowany proces dojrzałości procesów IT każdej firmy.
- Metodyka jest otwarta na powiązanie jej z innymi standardami, takimi jak ISO/IEC 38500, 31000, 27000, TOGAF, PMBoK/PRINCE2, CMM ITIL V3 2011 oraz ISO/IEC 20000.
- Ramy COBIT obejmują specjalistyczne przewodniki z wytycznymi w zakresie wdrożenia, bezpieczeństwa, audytu i zarządzania ryzykiem.
- Zastosowanie wytycznych COBIT zapewnia zgodność z obowiązującymi regulacjami ze względu na uwzględnienie niezbędnych elementów kontrolnych i aspektów bezpieczeństwa w procesach IT.
- Wykorzystanie COBIT pomaga audytorom identyfikować problemy z kontrolą IT w organizacji oraz potwierdzać wnioski audytowe.

WADY

- Praktyki COBIT koncentrują się na kontroli, a mniej na wykonaniu.
- COBIT stanowi rozbudowany i ambitny model, który wymaga dużej wiedzy specjalistycznej na etapie jego wdrożenia w organizacji.
- Zastosowanie COBIT może budzić obawy personelu ze względu na prawdopodobne możliwości wykrycia braków w obszarze zgodności z regulacjami i bezpieczeństwa oraz potencjalnie niskie oceny dojrzałości procesów IT.

