

## IT GOVERNANCE W PRZEDSIĘBIORSTWIE KOLEJOWYM

---

Ryszard Miłosz

mgr inż. CISA (Certified Information Systems Auditor) numer 0126044, tel.: +48 572 700 728

---

**Streszczenie.** Obecnie obszar kolejowy unowocześniając swoje możliwości w coraz większym stopniu do realizacji swoich celów wdraża rozwiązania informatyczne, które także w obecnych czasach nieustannie ulegają unowocześnieniu. Należy zaznaczyć, iż ciągle unowocześniania się informatyki odbywa się szybciej, niż w dowolnie innym wybranym obszarze i jest najszybsze w dziejach. Zastosowanie informatyki daje przedsiębiorstwom kolejowym przez to nowe, dużo lepsze możliwości, ale także ze względu na brak wcześniejszych doświadczeń stawia ogromne wyzwania. Dlatego też oprócz odgraniczania się do samego zarządzania technologiami IT bardzo istotnym obszarem w działalności przedsiębiorstwa jest nadzór nad technologiami informatycznymi. Nadzór pozwala uzyskać pewność, że właściwie oceniono potrzeby obszaru kolejowego w celu ustalenia zrównoważonych, uzgodnionych celów przedsiębiorstwa, które mają zostać osiągnięte w ramach zarządzania obszarem IT. Główne cele nadzoru nad obszarem IT to: realizacja korzyści, optymalizacja ryzyka, optymalizacja zasobów. Niniejszy artykuł w oparciu o metodykę audytu informatycznego COBIT 5 nakreśla na co należy zwrócić uwagę przy ustanawianiu nadzoru nad technologiami IT w przedsiębiorstwie kolejowym.

**Słowa kluczowe:** nadzór nad technologiami informatycznymi, COBIT, zarządzanie ryzykami IT w przedsiębiorstwie kolejowym, IT Governance

### 1. Wprowadzenie

Celem niniejszego artykułu jest nakreślenie zasad współpracy w przedsiębiorstwie kolejowym pomiędzy obszarami IT a kolejowym - odpowiedzialnym za obszar związany z funkcjonowaniem transportu kolejowego, utrzymaniem infrastruktury itp. Niemniej jednak opisane dalej zasady mogą zostać także wykorzystane jako drogowskaz w innych obszarach np. księgowości, kadrach itp. Jednakże w artykule położono większy nacisk na działalność kolejową ze względu na jej znacznie odmienną specyfikę w stosunku do obszarów bardziej biurowych. Przez działalność kolejową należy rozumieć prace związane z planowaniem ruchu kolejowego, jego realizacją, kierowaniem, sterowaniem i prowadzeniem ruchu pociągów, utrzymaniem bezpieczeństwa szlaków kolejowych oraz wszelkie inne związane z koleją.

Na wstępie należy jasno zaznaczyć, iż autor niniejszego artykułu nie jest kolejarzem a informatykiem, a właściwie już certyfikowanym audytorem informatycznych CISA (Certified Information Systems Auditor). Jednakże, mówiąc ogólnie głównym zadaniem audytora informatycznego jest ciągle zapewnianie, aby

potrzeby interesariuszy, w tym przypadku obszaru kolejowego, były możliwe jak najlepiej realizowane w obszarze IT. Niniejszy artykuł powstał w oparciu o audyty informatyczne realizowane w obszarach kolejowych, a przy ich okazji uzyskanych opinii od kolejarzy na temat wspomagania realizacji ich działań przez obszar IT, a dodatkowo przez udział autora w konferencjach poświęconych wykorzystaniu IT na kolei. W każdym z tych przypadków jasno było widać jakie jest obecnie duże znaczenie obszaru IT dla funkcjonowania przedsiębiorstwa kolejowego. Oznacza to nakreślenie właściwych zasad nadzoru w ramach przedsiębiorstwa kolejowego nad wykorzystywanymi technologiami IT, tj. IT Governance.

Artykułu tego nie należy więc traktować jako pracy dotyczącej jakichś aspektów związanych czysto z kolejnictwem, a wyłącznie wskazówek jak w przedsiębiorstwie kolejowym powinno się ułożyć zasady współpracy z obszarem IT. Wskazówek przekazywanych przez informatyka mającego nieco doświadczenia w kontaktach z kolejarzami, co jest zresztą zrozumiałe, gdyż w ten sposób można próbować nakreślić jak należy układać relacje z obszarem IT, aby uzyskać z jego posiadania jak najwięcej pożytku. Nie chodzi tutaj o narzucanie punktu widzenia IT na obszar kolejowy, wręcz odwrotnie - jak obszar kolejowy może informować o swoich potrzebach obszar IT i nakreślać pewne kierunki działania, niezbędne dla jego rozwoju.

## 2. Kolej a IT

Do podstawowej działalności przedsiębiorstwa kolejowego w zależności od jego charakteru może należeć zarządzanie infrastrukturą kolejową, prowadzenie ruchu pociągów, sterowanie ruchem, prowadzenie przewozów pasażerskich lub towarowych itp. Należy dodać, że podstawowe priorytety to bezpieczeństwo i punktualność ruchu. Należy także pamiętać, iż każde przedsiębiorstwo kolejowe tak jak inne, musi realizować swoje zadania w twardej rzeczywistości gospodarczej, tj. zarobić na swoje utrzymanie. Wymaga to prowadzenia jak największych i najszybszych przewozów, co stanowi niemałe wyzwanie dla wspomnianej wcześniej punktualności i bezpieczeństwa ze względu na wymagania do coraz większej szybkości i wydajności szlaków kolejowych. Coraz częściej mówi się o kolejach dużych prędkości. Generalnie pociągi poruszają się coraz szybciej, więc stare metody prowadzenia ruchu okazują się niewystarczające i są wykorzystywane w coraz mniejszym stopniu. Do tego celu wykorzystuje się w coraz większym stopniu informatykę. Obecne nowoczesne pojazdy kolejowe posiadają na wyposażeniu serwerownie, które muszą współpracować z innymi systemami IT wykorzystywanymi w kolejnictwie. Wprowadza się coraz więcej nowoczesnych rozwiązań, do których należą m.in. ERTMS, ETCS, GSM-R i wiele innych. Wykorzystanie informatyki w kolejnictwie niesie wiele pożytecznych aspektów, ale także stwarza nowe problemy. Z jednej strony zwiększa się prędkość i przepustowość dróg kolejowych, ale z drugiej strony, w przypadku wadliwego zadziałania systemów IT mogą powstać duże

opóźnienia lub może dojść do poważnych wypadków. Z obserwacji audytowych autora wynika, iż bardzo ważnym elementem unikania problemów, a jednocześnie czynnikiem coraz lepszej jakości funkcjonowania przedsiębiorstwa kolejowego jest sprawowanie właściwego nadzoru nad technologiami informatycznymi, tj. IT Governance. Dalsza część artykułu stara się dać praktyczną odpowiedź na pytanie jak w najbardziej optymalny sposób cel ten może zostać osiągnięty w przedsiębiorstwie kolejowym.

### 3. Metodyka audytu informatycznego COBIT

W latach 60 ubiegłego wieku następowało coraz większe wykorzystanie informatyki w wielu gałęziach gospodarki. Jednocześnie pojawiło się sporo problemów natury organizacyjnej, technicznej, a także różnego rodzaju nadużyć. W związku z tym pojawiły się oddolne inicjatywy zmierzające do próby rozwiązania problemów, z którymi biznes nie miał jeszcze do czynienia oraz znalezienia jakichś środków zaradczych. Inicjatywy te skupiały różne grupy zawodowe, głównie: audytorów finansowych i operacyjnych, informatyków, osoby z kierownictwa. Jedną z tych grup, która rozpoczęła działalność w 1967 r., a w 1969 r. sformalizowała swoją działalność jako Stowarzyszenie Audytorów EDP (EDP Auditors Association). W roku 1994 stowarzyszenie przekształciło się w Stowarzyszenie Audytu systemów informatycznych i kontroli (Information Systems Audit and Control Association ISACA). Obecnie ISACA działa w ponad 80 krajach i jest najważniejszą organizacją zrzeszającą audytorów informatycznych. Organizacja ISACA przyznaje dla osób zajmujących się audytem informatycznym certyfikat CISA (Certified Information System Auditor) uznawany także w Polsce, m.in. w Ustawie o finansach publicznych oraz Ustawie o krajowym systemie cyberbezpieczeństwa jako warunek umożliwiający nabycie uprawnień do przeprowadzania audytów informatycznych.

Od 1996 roku, po ciągłym zbieraniu doświadczeń związanych z funkcjonowaniem systemów informatycznych, a także coraz większym zastosowaniu informatyki w masowej obsłudze gospodarki, firm, ludności itp. ISACA wydaje metodykę audytu obszaru IT - COBIT (Control Objectives for Information and related Technology). COBIT stanowi zbiór dobrych praktyk i wskazówek z zakresu zarządzania procesami IT. Od 2012 roku wydano jego już piąte wydanie, w oparciu o które zostały zaczerpnięte wskazówki do nakreślenia zasad IT Governance w przedsiębiorstwach kolejowych, zwarte w niżej wymienionym artykule.

Jednakże przed opisaniem tych zasad, aby je lepiej zrozumieć, należy nieco włączyć się w COBIT. Przede wszystkim oparty on jest o wiele dziesięcioleci doświadczeń w obszarach związanych z wykorzystywaniem technologii informatycznych niezależnie od położenia geograficznego i różnych zastosowań. Nie próbuje więc on dostosować rzeczywistości do własnych wyobrażeń, ale daje zalecenia

w jaki sposób należy dostosować się do rzeczywistości aby uniknąć błędów, które zostały popełnione już wcześniej przez innych.

COBIT oparty jest o pięć podstawowych zasad:

**Zasada 1:** Spełnienie potrzeb interesariuszy - istotą działania przedsiębiorstwa jest tworzenie wartości dla interesariuszy poprzez zachowanie równowagi pomiędzy realizacją korzyści, optymalizacją ryzyka i wykorzystaniem zasobów. COBIT uwzględnia wszystkie wymagane procesy oraz inne czynniki umożliwiające, które wspierają tworzenie wartości biznesowej dzięki wykorzystaniu IT. W przypadku przedsiębiorstw kolejowych główną potrzebą jest realizacja ich celów statutowych związanych z ruchem kolejowym.

**Zasada 2:** Uwzględnienie wszystkich aspektów działania przedsiębiorstwa - nadzór nad technologiami informatycznymi w przedsiębiorstwie jest częścią ładu korporacyjnego:

- Obejmuje wszystkie funkcje i procesy realizowane w przedsiębiorstwie, nie tylko funkcje IT, ale traktuje informacje i związane z nimi technologie jako aktywa wymagające uwzględnienia - podobnie jak wszelkie inne zasoby.
- Wszystkie czynniki umożliwiające, dotyczące nadzoru nad systemami informatycznymi i zarządzania nimi są ogólnofirmowe i mają charakter kompleksowy, tj. obejmują wszystkich i wszystko — wewnątrz przedsiębiorstwa i poza nim — co jest istotne dla nadzoru nad zasobami informacyjnymi w przedsiębiorstwie i powiązаныmi systemami IT oraz zarządzania nimi.

Zasada ta oznacza, że nadzór nad procesami związanymi z obszarem kolejowym i wspierającymi je procesami z obszaru IT nie może być rozdzielony.

**Zasada 3:** Stosowanie jednej zintegrowanej metodyki - istnieje wiele standardów i dobrych praktyk związanych z IT, obejmujących wytyczne dotyczące poszczególnych zbiorów działań IT. Na poziomie ogólnym COBIT jest spójny z innymi stosowanymi standardami i metodykami. W związku z tym może on stanowić nadrzędną strukturę nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi.

**Zasada 4:** Wdrożenie podejścia całościowego - skuteczny nadzór nad technologiami informatycznymi oraz wydajne zarządzanie nimi w przedsiębiorstwie wymagają przyjęcia całościowego podejścia uwzględniającego wiele wzajemnie oddziałujących na siebie komponentów. COBIT definiuje zbiór czynników umożliwiających, które wspierają wdrożenie kompleksowego systemu nadzoru i zarządzania dla technologii informatycznych w przedsiębiorstwie. Czynniki umożliwiające to pojęcie bardzo szerokie - obejmuje wszystko, co może ułatwić osiągnięcie celów przedsiębiorstwa: W metodyce COBIT zdefiniowano siedem kategorii czynników umożliwiających:

- zasady, polityki i metodyki;
- procesy;
- struktury organizacyjne;
- kultura, etyka i zachowanie;
- informacja;
- usługi, infrastruktura i aplikacje;

- ludzie, umiejętności i kompetencje.

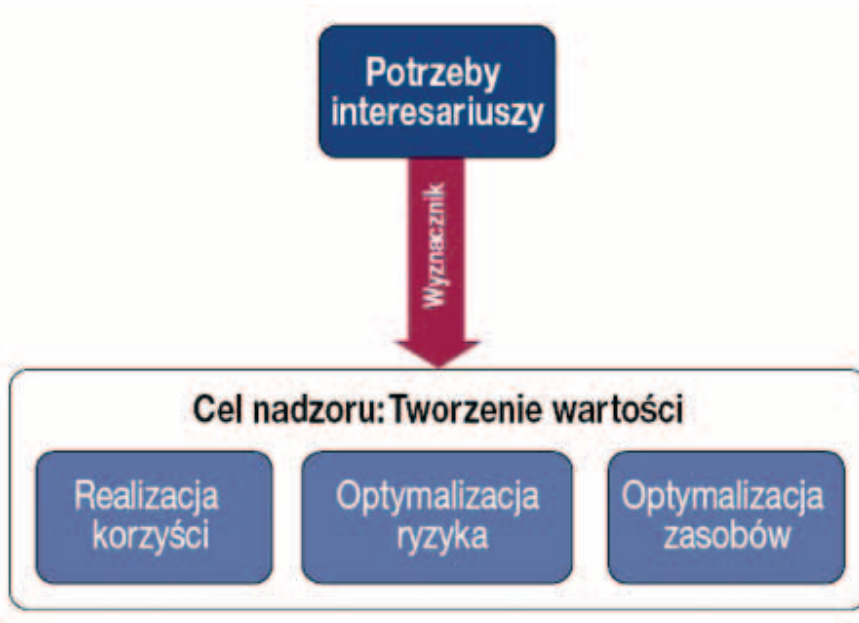
**Zasada 5:** Oddzielenie nadzoru od zarządzania - należy wyraźnie rozróżnić nadzór i zarządzanie. Każda z tych dziedzin obejmuje działania o odmiennym charakterze, wymaga różnych struktur organizacyjnych i służy innym celom. To kluczowe rozróżnienie nadzoru i zarządzania ujęto w następujący sposób, poprzez określenie ich celów funkcjonowania:

- Nadzór pozwala uzyskać pewność, że oceniono potrzeby, warunki i opcje interesariuszy w celu ustalenia zrównoważonych, uzgodnionych celów przedsiębiorstwa, które mają zostać osiągnięte. Polega on również na ukierunkowaniu działań poprzez nadanie priorytetów i podejmowanie decyzji, a także na monitorowaniu sprawności i zgodności w odniesieniu do uzgodnionego kierunku i szczegółowych celów.
- Zarządzanie polega na planowaniu, budowaniu, realizacji i monitorowaniu działań w sposób spójny z kierunkiem wskazanym przez nadzór IT, aby osiągnąć cele przedsiębiorstwa.

Należy to rozumieć, że zadaniem nadzoru nad technologiami informatycznymi jest ukierunkowanie działań obszaru IT w stronę jak najlepszego wsparcia działalności obszaru kolejowego, a nie wskazywanie działań zarządczych związanych z realizacją tego wsparcia – IT i kolej to są jednak nieco inne światy wymagające innych funkcji i procesów zarządczych. Nie należy także mylić nadzoru nad technologiami IT z nadzorem nad całym przedsiębiorstwem kolejowym, a w szczególności przypisywanie ściśle tego zadania do Rady Nadzorczej. W tym przypadku jest to przede wszystkim główne zadanie obszaru kolejowego oraz organów zarządzających przedsiębiorstwa kolejowego. Niemniej jednak nie istnieją żadne przeciwwskazania, aby nadzór ten był sprawowany w części lub przy udziale Rady Nadzorczej.

#### 4. COBIT – nadzór nad technologiami informatycznymi

Istotą funkcjonowania przedsiębiorstw kolejowych jest realizacja zadań związanych z ruchem kolejowym. Oznacza to, że dla każdego przedsiębiorstwa - jednym z celów w zakresie nadzoru jest tworzenie wartości w zakresie ruchu kolejowego. Może to być wartość związana z kierowaniem ruchu pociągów, prowadzeniem ruchu pasażerskiego, towarowego itp. Tworzenie wartości oznacza osiągnięcie korzyści w sposób maksymalnie oszczędny pod względem wykorzystania zasobów i umożliwiający optymalizację ryzyka. (rys. 1). Korzyści mogą przybierać wiele różnych postaci, np. mają charakter finansowy, zaś dla innych podmiotów są nimi usługi publiczne, tj. właśnie prowadzenie ruchu kolejowego.



Rys. 1. Realizacja zadań przedsiębiorstwa w zakresie nadzoru

Sprawowanie nadzoru nad technologiami IT powinno zmierzać w kierunku realizacji celów przedsiębiorstwa kolejowego. Jasno więc musi być określone:

- 1) Czy przedsiębiorstwo kolejowe uzyskuje jakieś korzyści ze stosowania technologii informatycznych. Może to być poprawa efektywności wykorzystania linii kolejowych, taboru kolejowego, poprawa punktualności itp.
- 2) Jak stosowanie technologii informatycznych wpływa na zagrożenia funkcjonowania obszaru kolejowego. Może to być np. system zarządzania bezpieczeństwem (SMS), pogorszenie punktualności, pogorszenie efektywności wykorzystania taboru itp. Jest to istotne szczególnie, iż to ryzyka informatyczne mają często bardzo duży wpływ na ryzyka związane z funkcjonowaniem kolei, a nie odwrotnie. Mogą one prowadzić do poważnych wypadków lub utrudnień w ruchu.
- 3) Czy obszar IT posiada zasoby umożliwiające realizację 2 poprzednich celów nadzoru. Także jest ważne, czy optymalizacja zasobów IT umożliwia optymalizację zasobów w obszarze kolejowym, a przez to poważną redukcję wydatków. Należy zaznaczyć, iż wydatki na IT w przypadku przedsiębiorstw kolejowych są znacznie niższe na zasoby związane z ruchem kolejowym np. pojazdów czy dróg kolejowych. Wprowadzanie nowoczesności w ruchu kolejowym wymaga znacznego unowocześniania obszaru IT, a tym samym kierowaniu do niego coraz to nowych i kosztownych zasobów np.: systemy, sprzęt, wykwalifikowany personel itp.

Cele nadzoru osiągnięte są w ramach realizacji kaskady celów (rys. 2). Najistotniejsze są cele interesariuszy, tu często potrzeby państwa w zakresie realizacji ruchu

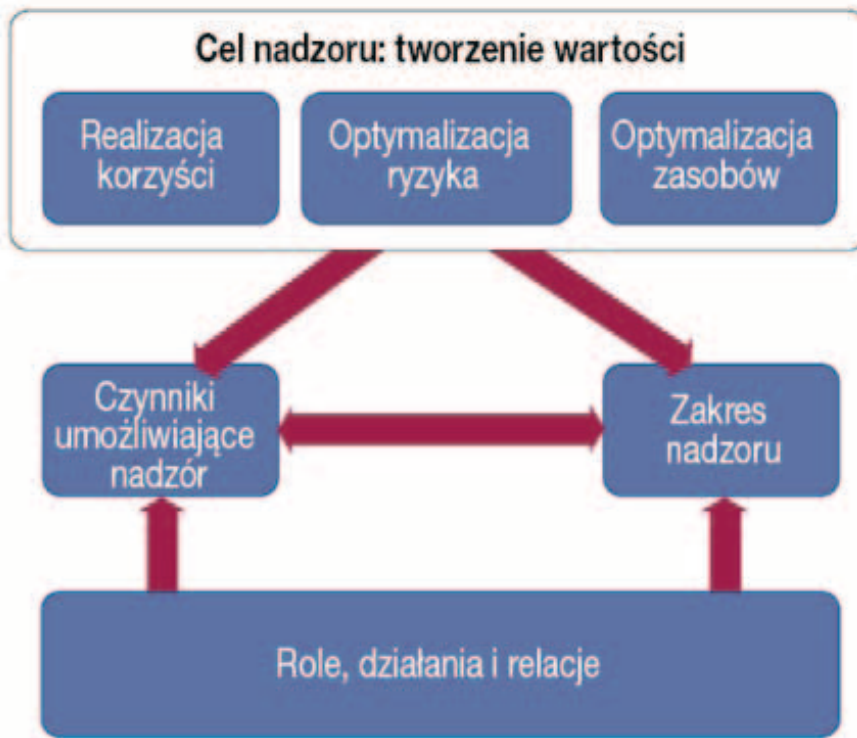
kolejowego, wyznaczenie celów dla przedsiębiorstwa kolejowego, celów związanych z IT w zakresie realizacji potrzeb kolejowych, a ostatecznie celów czynników umożliwiających. Cele związane z IT mogą stanowić np. stworzenie nowych funkcjonalności systemów kierowania ruchem kolejowym, informacji pasażerskiej itp.



Rys. 2. Kaskada celów

Sprawowanie nadzoru nad technologiami IT odbywa się poprzez wyznaczenie zakresu nadzoru oraz funkcjonowanie czynników umożliwiających nadzór (rys. 3).





Rys. 3. Sprawowanie nadzoru nad technologiami IT

Relacje nadzoru w stosunku do interesariuszy i zarządzania zostały ukazane na rys. 4.



Rys. 4. Relacje nadzoru w stosunku do interesariuszy i zarządzania

Głównym czynnikiem umożliwiającym sprawowanie nadzoru nad technologiami IT są właściwie określone i realizowane procesy nadzorcze. COBIT definiuje dobre praktyki w zakresie procesów związanych z IT dla 37 procesów, z czego 5 związanych z nadzorem, a 32 z zarządzaniem. W dalszej kolejności w artykule zostaną opisane praktyki dla procesów dotyczących nadzoru. Są to:

- 1) Zapewnienie utrzymania nadzoru nad technologiami IT.
- 2) Zapewnienie realizacji korzyści.
- 3) Zapewnienie optymalizacji ryzyka.
- 4) Zapewnienie optymalizacji zasobów.
- 5) Zapewnienie przejrzystości dotyczącej interesariuszy.



Należy zaznaczyć, że wszystkie wymienione powyżej procesy są ciągle. Tak samo jak nieustannie rozwija się technika kolejowa i nieustannie są doskonalone procesy związane z jej utrzymaniem i eksploatacją, tak samo muszą być traktowane procesy nadzoru nad technologiami IT. Cały czas przecież istotnym jest, aby osiągać z IT korzyści oraz generować jak najmniejsze ryzyka. Dlatego też należy zauważyć, że naprawdę nadzór nad technologiami IT zawsze w jakimś stopniu jest obecny, różny jest tylko stopień dojrzałości. Początkowo jest on realizowany nieformalnie i doraźnie, ale wraz z rozwojem przybiera ona bardziej dojrzały charakter. Dlatego należy pamiętać, że nigdy nie startuje się od samego początku i należy w ramach poprawiania nadzoru uwzględniać dotychczasowe doświadczenia.

Każdy z ww. procesów nadzorczych składa się z trzech etapów wykonywanych cyklicznie:

- 1) Ocena.
- 2) Realizacja.
- 3) Monitorowanie.

Prowadzenie cyklu ma za zadanie zapewnić, że nadzór nad IT będzie wykonywany w sposób optymalny, dostosowany do potrzeb przedsiębiorstwa kolejowego.

## 5. Zapewnienie utrzymania nadzoru nad technologiami IT

Najważniejsze aby nadzór nad technologiami IT był w przedsiębiorstwie kolejowym ustanowiony, gdyż tylko w tym przypadku możliwe jest efektywne wsparcie obszaru kolejowego ze strony IT, należy wiele uwagi i troski włożyć w jego właściwe ustanowienie i umiejscowienie. Celem tego procesu jest więc ocena potrzeb w zakresie nadzoru nad technologiami IT w przedsiębiorstwie kolejowym, a następnie ustanowienie jego w wymaganym zakresie. Nadzór ten powinien być realizowany poprzez jasno określone struktury organizacyjne przy jasno określonych zadaniach, obowiązkach i odpowiedzialnościach. Powinny zostać zidentyfikowane pryncypia, praktyki i wynikające z nich procesy niezbędne do osiągnięcia misji, celów i planów przedsiębiorstwa.

Ustanowienie nadzoru z kolei umożliwi strukturom IT w przyszłości dopasowanie swojej strategii do strategii przedsiębiorstwa, zwiększenie zaangażowania najwyższego kierownictwa w obszarze IT, a najważniejsze - dostarczanie usług informatycznych wspierających działalność kolejową zgodnie z zapotrzebowaniem.

### 1) Ocena

Na tym etapie należy zrozumieć własne potrzeby i zadania, które należy realizować w zakresie nadzoru nad technologiami IT. W tym celu należy zidentyfikować wszelkie istotne czynniki zewnętrzne i wewnętrzne mające wpływ na funkcjonowanie obszaru kolejowego. W przypadku kolei bardzo istotne jest otoczenie prawne oraz inne uregulowania związane z ruchem kolejowym. Należą do nich np. Ustawa o transporcie kolejowym i inne powiązane uregulowania, Ustawa o cyberbezpieczeństwie – nakłada obowiązki na zarządcę infrastruktury i przewoźników,

System Zarządzania Bezpieczeństwem SMS, dodatkowo olbrzymia liczba innych uregulowań, norm, standardów itp., nierzadko bezpośrednio niezwiązanymi z obszarem kolejowym np. ochrona danych osobowych itp.

W dalszej kolejności należy ocenić rolę IT w realizacji działalności przedsiębiorstwa kolejowego, a także w przypadku spełnienia wymogów zidentyfikowanych powyżej. Należy ocenić także niekorzystny wpływ w jaki sposób IT może wpływać na działalność przedsiębiorstwa w przypadku wystąpienia różnych problemów.

Poprzednie oceny dają możliwość oszacowania, czy obecnie sprawowany nadzór nad technologiami IT dostosowany jest do działalności przedsiębiorstwa kolejowego i czy jest on właściwie praktykowany w przedsiębiorstwie, tj. czy nadzór nad IT wynika z nadzoru nad całym obszarem kolejowym. Można więc właściwie określić wymagane pryncypia i kierunki zmian, które komórki, w jakim zakresie i z jakimi uprawnieniami będą prowadziły nadzór. Należy nie zapominać, że w przypadku przedsiębiorstwa kolejowego należy głęboko rozważyć, które części obszaru kolejowego powinny brać udział w sprawowaniu nadzoru nad IT. Błędem jest przypisywanie tego zadania wyłącznie do części przedsiębiorstwa odpowiedzialnych za kadry, finanse, marketing, public relations, itp. W tym przypadku środowisko IT będzie miało bardzo utrudnione uruchomienie działań zarządczych do realizacji potrzeb w obszarze kolejowym.

## 2) *Realizacja*

Przeanalizowanie potrzeb w zakresie nadzoru nad IT umożliwia ocenę, czy nadzór realizowany jest obecnie w wymaganym zakresie, czy jest dostosowany potrzeb przedsiębiorstwa kolejowego, a w dalszej kolejności przeprowadzenie niezbędnych zmian i właściwą realizację IT Governance.

Rozwiązania mogą być różne. Czasami może wystarczyć sprawowanie nadzoru bezpośrednio przez Zarząd, jednakże najczęściej stosowanym jest powoływanie wewnątrzorganizacyjnego ciała, np. typu Rada informatyzacji. Prace rady mogą być wspomagane przez konsultantów, specjalistów zewnętrznych itp. W przypadku zarządcy infrastruktury istotne role powinny pełnić komórki odpowiedzialne za bezpieczeństwo, prowadzenie lub sterowanie ruchem kolejowym. W przypadku przewoźników komórki odpowiadające za planowanie przewozów, utrzymanie taboru itp.

## 3) *Monitorowanie*

Wraz z rozwojem kolejnictwa i innych czynników zmieniają się także uwarunkowania i wynikające z nich potrzeby. Należy dodać, że tak samo zmieniają się możliwości IT oraz rośnie zakres i możliwości jego stosowania. Nowoczesne drogi kolejowe oraz kursujące po nich pojazdy kolejowe są w coraz większym stopniu wyposażane w najnowsze rozwiązania informatyczne. Obszar kolejowy i IT stają przed coraz to trudniejszymi wyzwaniami. Nigdy nie ma gwarancji, że nadzór nad technologiami IT jest sprawowany optymalnie lub nie może być sprawowany lepiej. Należy więc monitorować jego efektywność.

Głównym kryterium monitorowania jest ciągła i okresowa ocena funkcjonowania nadzoru. Czy decyzje nie są podejmowane zbyt późno, czy są podejmowane właściwie, czy obszar IT właściwie realizuje potrzeby przedsiębiorstwa, czy dostaje jasne wymagania, które mogą zostać zrealizowane. Najważniejszym kryterium jest dobra ocena przez obszar kolejowy. Dobrą praktyką jest przeprowadzanie niezależnych ocen IT Governance, szczególnie audytów.

## 6. Zapewnienie realizacji korzyści

Bez uzyskiwania realnych korzyści z technologii informatycznych nie ma sensu ich stosowania. Przy czym nie są istotne korzyści wynikające z samego faktu posiadania IT, że stosujemy, np. tak jak inni nowocześniejsze rozwiązania, ale te ściśle związane z funkcjonowaniem przedsiębiorstwa kolejowego, realizowania jego misji i celów, oraz uzyskiwania korzyści biznesowych.

Dlatego też należy zabezpieczyć uzyskiwanie korzyści dla obszaru kolejowego z realizowanych inicjatyw IT, świadczonych usług i z posiadanych zasobów IT. Z powodu specyfiki obszaru kolejowego nie tylko istotne są korzyści finansowe, tutaj także ważna jest relacja korzyści dla obszaru kolejowego w stosunku do kosztów funkcjonowania IT. Im wyższa tym lepiej.

### 1) Ocena

W tym celu należy zrozumieć jakie są obecne i przyszłe potrzeby obszaru kolejowego, co stanowi o ich wartości oraz jakie w związku z tym są ich wymagania. Może to być bezpieczeństwo, punktualność, zwiększona przepustowość szlaków poprzez lepsze kierowanie i sterowanie ruchem pociągów, a w następstwie większe wpływy finansowe.

W tym przypadku obszar IT może mieć też swoją rolę aktywną czyli identyfikować nowe możliwości technologii informatycznych, a tym samym polepszać istniejące lub kreować nowe obszary działalności.

Bardzo ważna jest ocena jak obszar IT wspiera plany i strategie działalności przedsiębiorstwa. Czy wprost strategia IT wynika ze strategii przedsiębiorstwa i czy daje określone korzyści.

### 2) Realizacja

Należy wprowadzić właściwe zasady i praktyki nadzorcze nad technologiami IT ukierunkowujące działalność IT na wsparcie w realizacji oczekiwanych korzyści dla przedsiębiorstwa kolejowego.

W tym celu należy ocenić istniejące zasady prowadzenia wszelkich inwestycji i projektów IT oraz świadczenia usług IT. W ramach nadzoru musi być określona konieczność uzyskiwania określonych korzyści. Przed uruchomieniem wszelkich działań obszar kolejowy powinien je szacować. W ramach nadzoru należy oceniać uzyskane wyniki. Nadzór musi także ukierunkowywać IT na działania innowacyjne.

### 3) *Monitorowanie*

Uzyskiwanie korzyści z funkcjonowania IT monitoruje się poprzez określenie stosownych miar, wskaźników, celów, benchmarków oraz ich analizowanie w wymaganych interwałach czasowych. Muszą one odnosić się do zakładanych korzyści i realizacji celów pozwalających na ich uzyskanie.

W przypadku IT będzie to osiąganie określonych celów pozwalających na spełnienie wymagań obszaru kolejowego w następstwie czego uzyskiwane będą oczekiwane korzyści np. lepsza gospodarka pojazdami kolejowymi, bezpieczeństwo SMS itp. Monitorować należy parametry wyłącznie ściśle związane z realizacją korzyści biznesowych. Błędem jest posługiwanie się bezpośrednio miarami informatycznymi bez odniesienia do korzyści dla przedsiębiorstwa kolejowego np. nie zakupiliśmy 10 nowych serwerów, ale w jaki sposób usprawniło się np. kierowanie ruchem pociągów. Inaczej prowadzi to do niewłaściwej oceny.

Wszelkie zauważone niekorzystne odchylenia powinny prowadzić do adekwatnych działań naprawczych.

## 7. Zapewnienie optymalizacji ryzyka

W przypadku ruchu kolejowego nadrzędne jest jego bezpieczeństwo. Dodatkowo bardzo istotnym elementem jest bezpieczeństwo prowadzenia różnorodnych kolejowych działań operacyjnych, oraz ryzyka powiązane z osiągnięciem zakładanych celów. W przypadku wsparcia przez technologie oraz procesy IT, mogą one samym swoim udziałem spowodować zwiększenie ryzyk powiązanych z realizacją celów kolejowych w coraz to poważniejszym stopniu. Dlatego też jednym z najbardziej kluczowych celów nadzoru nad technologiami IT jest to że ryzyko związane z wykorzystaniem IT nie spowoduje przekroczenia dopuszczalnych granic dla ryzyk kolejowych. Ponadto negatywne wpływy ryzyk IT na realizację celów powinny być znane i zarządzane, a wszelkie potencjalne skutki zminimalizowane do stanu akceptowalnego.

Cel nadzoru nad technologiami IT w tym przypadku zapewnienia minimalizacji ryzyka zostanie osiągnięty jeżeli:

- prognozy ryzyk zostały zdefiniowane oraz powiązane ryzyka IT są znane,
- przedsiębiorstwo kolejowe zarządza ryzykami IT skutecznie i efektywnie,
- ryzyka IT nie przekraczają ustalonych progów i wpływ ryzyk IT na działalność przedsiębiorstwa kolejowego został zidentyfikowany i jest zarządzany.

### 1) *Ocena*

Należy ocenić efekty ryzyk IT na działalność przedsiębiorstwa kolejowego. Obecnie przy bardzo dużym wsparciu funkcjonowania kolei przez technologie IT niewątpliwie wpływ ten jest ogromny. W przypadku wielu gałęzi gospodarki możliwe są duże straty finansowe, a tutaj dodatkowo może skończyć się np. dłuższymi przestojami pasażerskimi lub poważnymi wypadkami kolejowymi. Ważne

jest określenie dopuszczalnego poziomu tych ryzyk. Np. w przypadku transportu pasażerskiego zgodnie z Ustawą o cyberbezpieczeństwie jest przerwanie świadczenia usługi na 2 godziny lub uszkodzenie systemów informacyjnych kluczowych dla sterowania i funkcjonowania pojazdu szynowego. Potrzeby szacuje się nie tylko w oparciu o wymagania ustawowe, ale także własne dla przedsiębiorstwa kolejowego.

Ostatecznie niezbędne jest oszacowanie dopuszczalnych poziomów ryzyk oraz określenie na nie wpływu technologii IT. W dalszej kolejności należy określić jakie czynniki ryzyka przyczyniają się do ich powstania. Ostatecznie można zidentyfikować jakie obszary działalności przedsiębiorstwa należy objąć zarządzaniem ryzykiem IT oraz jakie w tym kierunku powinny zostać wdrożone właściwe działania. Ostatecznie można ocenić obecnie funkcjonujące zarządzanie ryzykiem w przedsiębiorstwie kolejowym.

### 2) *Realizacja*

W dalszej kolejności powinno nastąpić, jeżeli to niezbędne, wdrożenie lub usprawnienie procesu zarządzania ryzykami IT w przedsiębiorstwie kolejowym. Należy pamiętać, iż zarządzanie ryzykami IT musi być zintegrowane z procesami wspieranymi przez technologie IT. Niemożliwe jest np. zarządzanie ryzykiem przewozów bez powiązania z systemami IT wspierającymi ten proces. Powinny zostać zaimplementowane odpowiednie mechanizmy komunikacyjne, odpowiedzi na zmiany ryzyk, eskalacji działań. Należy także zdefiniować odpowiednie cele kluczowe oraz metryki dla procesu zarządzania ryzykiem.

### 3) *Monitorowanie*

Zarządzanie ryzykiem w przedsiębiorstwie kolejowym powinno być nieustannie monitorowane. Jest to wymóg związany przede wszystkim z bardzo szybko postępującą informatyzacją oraz ciągłym monitoringiem sytuacji na szlakach kolejowych. Należy jeszcze wspomnieć o planowanych inwestycjach, np. w koleje duże prędkości. W tej sytuacji nadzór nad zapewnieniem optymalizacji ryzyka powinien zmierzać do udoskonalania procesu zarządzania ryzykami IT. W celu sprawowania właściwego nadzoru należy: monitorować obszar zarządzania ryzykiem IT w stosunku do przyjętych dopuszczalnych poziomów ryzyk, realizację celów kluczowych i wartości zdefiniowanych metryk. Bardzo ważne jest zaangażowanie obszaru kolejowego, gdyż jak wspomniano wcześniej skutki w maksymalnym stopniu mogą dotknąć właśnie ten obszar.

## 8. Zapewnienie optymalizacji zasobów

Obszar IT w celu wspierania pracy obszaru kolejowego i innych musi posiadać niezbędne zasoby i zdolności do realizacji procesów IT wspierających procesy kolejowe. Do zasobów tych należy kadra informatyczna, sprzęt, oprogramowanie,

licencji itp. Celem nadzoru jest zapewnienie, aby zasoby te były dostępne w ilości optymalnej do stawianych zadań. W przypadku przedsiębiorstw kolejowych powszechnym zjawiskiem jest to, że koszty funkcjonowania IT stanowią z reguły bardzo niewielką część kosztów funkcjonowania obszaru kolejowego. Ponadto ciągły rozwój technologii IT umożliwia coraz lepszą i wydajniejszą pracę obszaru kolejowego, a także optymalizację zasobów i kosztów jego działalności, co też niewątpliwie należy uwzględnić.

Cel nadzoru zostanie osiągnięty gdy:

- potrzeby przedsiębiorstwa kolejowego na niezbędne zasoby IT są zaspokojone w sposób optymalny,
- zasoby te są przydzielone w sposób najlepiej zaspokajający te potrzeby z uwzględnieniem ograniczeń kosztowych,
- optymalne wykorzystywanie zasobów odbywa się w całym ich cyklu życia.

### 1) *Ocena*

Jest to ważny etap w którym nadzór powinien nieustannie sprawdzać i oceniać bieżące i przyszłe zapotrzebowanie na zasoby IT, opcje zaspokajania potrzeb, przydział i zarządzanie nimi, aby zaspokoić je jak najkorzystniej z punktu widzenia przedsiębiorstwa kolejowego. Błędy popełnione na tym etapie mogą w znacznym stopniu wpływać na zaspokajanie bieżących i przyszłych potrzeb na wspieranie przez IT działalności kolejowej oraz jakość tego wsparcia.

Najlepszą praktykę w tym zakresie stanowi:

- rozważanie opcji nabywania zasobów IT w oparciu o strategię przedsiębiorstwa, jego bieżące i przyszłe potrzeby; strategia IT powinna wynikać ze strategii przedsiębiorstwa,
- nakreślenie pryncypiów, którymi należy kierować się przy przydziale i zarządzaniu nimi,
- krytyczna ocena i aprobatą planu nabywania zasobów oraz możliwych strategii realizacji tego planu,
- oszacowanie wymagań związanych z zarządzaniem zasobami IT w stosunku do zarządzania finansowego i zasobami ludzkimi,
- zdefiniowanie w razie konieczności wynikających z rozwojem środowiska IT nowych pryncypiów zarządzania i kontroli środowiska IT.

### 2) *Realizacja*

Na tym etapie należy wdrożyć pryncypia, nadzorować realizację strategii:

- zakomunikować i nadzorować strategię zarządzania zasobami, ustalone pryncypia i plan nabywania zasobów,
- przypisać stosowne odpowiedzialności,
- zdefiniować cele kluczowe, miary i metryki w stosunku do zarządzania zasobami,
- określić pryncypia pieczy nad zasobami,
- dopasować zarządzanie zasobami do zarządzania finansowego i HR.

### 3) *Monitorowanie*

Ten etap nie tylko polega na monitorowaniu postępów realizacji w stosunku do środowiska IT, jest także niezmiernie ważny ze względu na fakt, iż planowane potrzeby obszaru kolejowego mogą także ulegać zmianie, na co należy zwrócić uwagę z wyprzedzeniem. Dobrą praktykę stanowi tutaj monitorowanie:

- zgodności przydziału zasobów w stosunku do potrzeb przedsiębiorstwa i przyjętych priorytetów, uwzględniając uzgodnione kluczowe cele i metryki,
- realizację strategii przedsiębiorstwa i wynikającą z niej strategię IT, czy potrzeby przedsiębiorstwa zostaną zaspokojone,
- funkcjonowanie zasobów IT w stosunku do zakładanych celów, analizowanie przyczyn odchyżeń i przebieg podjętych akcji naprawczych.

## 9. Zapewnienie przejrzystości dotyczącej interesariuszy

Nawet najlepsze zarządzanie obszarem IT może nie dawać większych korzyści dla interesariuszy, jeżeli aspekt wzajemnej komunikacji, a zwłaszcza możliwości zrozumienia działań podejmowanych przez IT w interesie interesariuszy jest niewystarczający. Problem ten dla obszaru kolejowego jest bardzo istotny. Biorąc pod uwagę potencjalne korzyści oraz fakt, że obecnie bez wykorzystania informatyki w kolejnictwie trzeba by się było cofnąć do poprzedniej epoki, należy jasno wskazać że obszar IT nie stanowi w stosunku do obszaru kolejowego jednostki usługowej, ale jest pełnoprawnym partnerem w zapewnieniu przewozów kolejowych.

Dlatego też bardzo istotne jest zapewnienie przejrzystości dla interesariuszy, polegające na tym, że komunikacja z nimi jest podejmowana w sposób efektywny, skuteczny i w wymaganym przedziale czasowym. Zasady komunikacji (informowanie, raportowanie itp.) są ustanowione w sposób ułatwiający poprawę efektów wsparcia działań IT dla obszaru kolejowego, identyfikację obszarów wymagających poprawy i zapewnienia, że cele IT będą zbieżne ze strategią działania obszaru kolejowego.

Można uznać, że cele są osiągnięte jeżeli komunikacja ta jest: zgodna z potrzebami obszaru kolejowego, odbywa się w wymaganym czasie, jest poprawna i kompletna, jest efektywna i dobrze oceniana przez obszar kolejowy. W przeciwnym wypadku istnieje ryzyko zajścia wielu zdarzeń niepożądanych w obszarze kolejowym np. zagrożenie bezpieczeństwa, punktualności, efektywnego wykorzystania taboru i innych zasobów.

### 1) *Ocena*

Należy nieustannie szacować obecne i przyszłe potrzeby komunikacji i raportowania włączając w to obligatoryjne wymogi prawne i wymogi dla interesariuszy zewnętrznych. Przykładowo może to być raportowanie w przypadku wystąpienia incydentu opisanego w Ustawie o krajowym systemie cyberbezpieczeństwa, ra-



portowanie wewnątrz przedsiębiorstwa kolejowego o przestojach systemów kierowania ruchem itp. Należy określić pryncypia włączając w to kanały i formaty komunikacji, a także właściwe procedury akceptacji.

### 2) *Realizacja*

Realizacja komunikacji i raportowania powinna funkcjonować w oparciu o właściwe mechanizmy kontrolne. W przypadku niewydolności działań konieczne jest ustanowienie odpowiednich mechanizmów eskalowania problemów.

### 3) *Monitorowanie*

Przy monitorowaniu komunikacji należy oceniać funkcjonowanie mechanizmów zapewniających osiągnięcie zakładanych celów. Należy zwrócić uwagę, że funkcjonowanie komunikacji należy zawsze monitorować w ramach procesów, z którymi jest związana, zwłaszcza jeżeli jest ściśle powiązana bezpośrednio z działaniami kolejowymi.

## Bibliografia

- [1] COBIT® 5: A Business Framework for the Governance and Management of Enterprise IT.
- [2] COBIT® 5: Enabling Processes.