Dariusz Kralewski[*]

Ład informatyczny w oparciu o normę ISO/IEC 38500

Wstęp

Funkcjonowanie efektywnego systemu ładu korporacyjnego w przedsiębiorstwie jak i w całej gospodarce pomaga osiągnąć taki poziom zaufania, jaki jest niezbędny do funkcjonowania gospodarki rynkowej [OECD, 2004]. Ład korporacyjny jest procesem, w którym rada nadzorcza, poprzez kierownictwo, wspomaga instytucję w wypełnianiu misji i ochronie majątku. Efektywny ład korporacyjny ma miejsce, gdy zarząd przekazuje odpowiednie wskazówki dla kierownictwa zawierające strategiczne kierunki instytucji i nadzoruje wysiłki kierownictwa dążenia w tym kierunku [Rock, Otero, Saltyman 1998]. W ostatnich latach technologie informatyczne stały się szkieletem przedsiębiorstw. Dla wielu z nich byłoby niemożliwym funkcjonowanie bez IT. Technologie informatyczne nie są obecnie odseparowane od przedsiębiorstwa, są jego istotnym elementem. Kadra kierownicza w niedalekiej przeszłości mogła delegować, ignorować lub unikać decyzji związanych z IT. Obecnie w większości firm jest to niemożliwe [Grembergen, DeHaes, 2005]. Brak nadzoru zarządu nad działaniami IT jest niebezpieczne; naraża przedsiębiorstwo na ryzyko w ten sam sposób, jak brak badania ksiąg rachunkowych [Nolan, McFarlen, 2005]. Bank Rozrachunków Międzynarodowych (Bank for International Settlements (BIS)) wskazał, że członkowie zarządu w instytucjach finansowych powinni skupiać się na IT w takim samym stopniu, jak na każdych innych strategicznych punktach [BIS, 1999]. Bezwzględne uzależnienie od technologii informacyjnych zmusza do szczególnej koncentracji na ładzie informatycznym (IT governance) w celu zapewnienia, że inwestycje w IT wygenerują żądaną wartość biznesową a ryzyka związane z IT zostaną zminimalizowane [ITGI, 2011]. Głównym celem tego artykułu jest prezentacja kluczowych pojęć ładu informatycznego, opis najważniejszych modeli (*frameworks*) ładu informatycznego stosowanych przez organizacje, a także sprecyzowanie wytycznych dla organizacji w celu skutecznego, efektywnego i zyskownego wykorzystania IT bazując o normę ISO / IEC 38500:2008

[*] Dr, Katedra Informatyki Ekonomicznej, Wydział Zarządzania, Uniwersytet Gdański, darek@univ.gda.pl

[ISO/IEC, 2008]. Artykuł ten powinien pomóc członkom zarządu implementować ład informatyczny.

1. Elementy ładu informatycznego

IT Governance Institute (ITGI) stwierdza, że ład IT zasadniczo skupia się na dwóch płaszczyznach: dostarczaniu przez IT wartości firmie i łagodzeniu zagrożeń wynikających ze stosowania IT. Pierwszy element uzyskiwany jest przez strategiczne dostosowywanie IT z biznesem. Drugi element jest osiągany przez wprowadzenie rozliczalności w przedsiębiorstwie. Obie płaszczyzny muszą być wspierane przez odpowiednie zasoby i mierzone dla zapewnienia uzyskiwanych wyników.

Powyższe płaszczyzny, z punktu widzenia interesariuszy, prowadzą do wyszczególnienia pięciu głównych obszarów tematycznych ładu informatycznego. Dwa z nich są wynikiem analizy: dostarczania wartości i zarządzania ryzykiem. Trzy z nich są realizacją: dopasowania strategicznego, zarządzania zasobami i pomiaru wyników. IT governance jest ustawicznym cyklem życia [ITGI, 2003].

Rysunek. 1. Obszary tematyczne ładu informatycznego

Źródło: Opracowanie własne.

Dopasowanie strategiczne skupia się na zapewnieniu powiązania biznesu i planów IT, na definiowaniu, utrzymywaniu i walidacji wartości propozycji IT i koordynowaniu operacji IT z operacjami przedsiębiorstwa. Dopasowanie strategiczne koncentruje się na decyzjach inwestycyjnych i realizacji optymalnych korzyści z IT. Polega ono na prezentacji i zatwierdzeniu wartościowych propozycji IT. Dopasowanie strate-

giczne gwarantuje jasne powiązania między strategią przedsiębiorstwa, portfelem programów inwestycyjnych w IT, które realizują strategię, poszczególnych programów inwestycyjnych, projektów IT i biznesowych, które tworzą programy. Jest on oparty na założeniu, że wartość z IT jest osiągana tylko wtedy, gdy inwestycje związane z IT są zarządzane jako portfolio programów, które obejmuje cały zakres zmian, jakie firma musi podjąć w celu optymalizacji wartości z możliwości które oferuje IT w realizacji strategii. Dopasowanie strategiczne zwiększa zrozumienie i przejrzystość kosztów, ryzyka i korzyści wynikających ze znacznie bardziej świadomych decyzji kierownictwa. To zwiększa prawdopodobieństwo wyboru inwestycji, które mają potencjał wygenerowania największego zysku i zwiększa prawdopodobieństwo sukcesu wykonania wybranych inwestycji, tak aby osiągnąć lub przekroczyć zwrot z inwestycji. Dopasowanie strategiczne obniża koszty poprzez nierobienie rzeczy, których nie powinno się robić i podejmowanie działań naprawczych już na początku lub zakończenie inwestycji, które nie dostarczają oczekiwanego potencjału. Zmniejsza ryzyko awarii, szczególnie awarii, które mają wysoki negatywny wpływ na przedsiębiorstwo. Wreszcie zmniejsza niespodzianki związane z kosztami i realizacją IT, w ten sposób zwiększając wartość biznesową, ograniczając zbędne koszty i zwiększając ogólny poziom zaufania do IT [Woźniak, 2012].

Dostarczanie wartości mówi o wykonywaniu wartościowych propozycji w całym cyklu realizacji, sprawiając, że IT dostarcza obiecane korzyści w stosunku do strategii, koncentrując się na optymalizacji kosztów, udowodnianiu wartości IT, i nadzorowaniu projektów i procesów operacyjnych korzystając z praktyk, które zwiększają prawdopodobieństwo sukcesu (jakość, ryzyko, czas, budżet, koszty, itp.) . Dostarczanie wartości umożliwia zarządzanie programami inwestycyjnymi związanymi z IT i innymi aktywami i usługami IT w celu zapewnienia że dostarczają jak największej wartości w wspieraniu strategii i celów przedsiębiorstwa. Zapewnia, że oczekiwane wyniki biznesowe inwestycji związanych z IT, i pełen zakres wysiłków potrzebnych do osiągnięcia tych rezultatów jest zrozumiały; że kompleksowe i spójne przypadki biznesowe są tworzone i zatwierdzone przez zainteresowane strony; że aktywa i inwestycje są zarządzanych przez cały cykl ekonomiczny; i że prowadzone jest aktywne zarządzanie realizowanymi korzyściami, takie jak poszerzanie nowych usług, zwiększenie efektywności i szybsze reagowanie na potrzeby klientów. Dostarczanie wartości wymusza zdyscyplinowane podejście do zarządzania portfolio, programami i projek-

tami, nalegając, żeby firma przejęła na własność wszystkie inicjatywy biznesowe związane z IT i że IT gwarantuje optymalizację kosztów realizacji zadań i usług IT. Zapewnia, że inwestycje w nowe technologie są standaryzowane w największym możliwym stopniu, tak aby uniknąć wzrostu kosztów i mnożenia złożoności rozwiązań technicznych.

Zarządzanie zasobami skupia się na optymalizacji inwestycji, wykorzystaniu i podziale zasobów IT (procesów, ludzi, aplikacji, technologii, urządzeń, infrastruktury, danych) w obsłudze potrzeb przedsiębiorstwa, przy jednoczesnej maksymalizacji efektywności tych aktywów i optymalizacji ich kosztów. Kluczowe zagadnienia odnoszą się do optymalizacji wiedzy i infrastruktury. Optymalizacja inwestycji, wykorzystanie i alokacja zasobów IT jest osiągana poprzez regularne oceny, sprawdzające, że IT posada wystarczające, kompetentne i stosowne zasoby do realizacji obecnych i przyszłych celów strategicznych i jest w stanie sprostać wymaganiom biznesowym. Jasne, spójne i egzekwowane polityki i mechanizmy zamówień muszą być ratyfikowane i zinstytucjonalizowane, tak aby zapewnić że wymagania dotyczące zasobów są efektywnie i zgodnie z architekturą polityk i standardów. Infrastruktura IT powinna być okresowo oceniana pod względem, tam gdzie to jest możliwe standaryzacji a gdzie jest to wymagane interoperacyjności. Kluczowym wyzwaniem zarządzania zasobami jest wiedza, gdzie i jak korzystać z zasobów zewnętrznych oraz wiedza, jak zarządzać usługami pozyskanymi z zewnątrz tak, aby dostarczały gwarantowane usługi po akceptowalnej cenie. Zarządzanie zasobami sprawia, że wiedza jest przechowywana i udostępniana w całej firmie.

Zarządzanie ryzykiem wymaga świadomości ryzyka, jasnego zdefiniowania apetytu przedsiębiorstwa na ryzyko i przejrzystości na temat znaczących ryzyk dla przedsiębiorstwa i osadzanie obowiązku zarządzania ryzykiem w organizacji. Zarządzanie ryzykiem jest kierowane w szczególności dla ochrony aktywów IT, odtwarzania po awarii i zapewnienia ciągłości działania. Należy ustanowić szkielet oceny ryzyka w celu utworzenia spójnego i kompleksowego podejścia do zarządzania ryzykiem dla IT w kontekście zarządzania ryzykiem całego przedsiębiorstwa. Powinien on obejmować regularną ocenę odpowiednich zagrożeń dla realizacji celów biznesowych, stanowiąc podstawę ustalenia, jak należy zarządzać ryzykiem, do uzgodnionego poziomu. Apetyt ryzyka przedsiębiorstwa na ryzyka IT powinien zostać określony i ogłoszony w zgodzie z planem zarządzania ryzykiem. Obowiązki w zakresie zarządzania ryzykiem powinny być wbudowane w organizację, zapew-

niając, że biznes i IT regularnie oceniają i raportują ryzyka związane z IT i ich wpływ na biznes. Zarządzanie IT powinno obserwować ekspozycje ryzyka, zwracając szczególną uwagę na kontrolę niepowodzeń IT i na słabe strony w kontroli wewnętrznej i nadzorze oraz ich rzeczywisty i potencjalny wpływ na biznes. Pozycja ryzyka IT przedsiębiorstwa powinna być przejrzysta dla wszystkich zainteresowanych stron.

Pomiar wyników śledzi i monitoruje strategię wdrażania, realizacji projektu, wykorzystania zasobów, wydajności procesów i świadczenia usług, za pomocą, na przykład, zrównoważonej karty wyników, która przekłada strategię na działania zmierzające do osiągnięcia mierzalnych celów poza ogólnie przyjętymi zasadami rachunkowości, pomiaru tych relacji i opartych na wiedzy aktywów niezbędnych do konkurowania w erze informacji: orientacji na kliencie, efektywności procesów i zdolność do uczenia się i rozwoju. Odpowiednie portfolio, program i działania IT powinny być zgłaszane do zarządu szybko i dokładnie. Raporty zarządcze powinny być dostarczone do recenzji kierownictwa wyższego szczebla przedsiębiorstwa ukazując postęp w osiąganiu określonych celów. Raporty o stanie powinny zawierać rozwinięcie, które planowane cele zostały zrealizowane, jakie uzyskano wyniki, czy spełniono cele pomiaru i czy zmniejszono ryzyka. Powinno dążyć się do integracji raportowania podobnych funkcji biznesowych. Miary wyników powinny zostać zatwierdzone przez kluczowych interesariuszy. Zarząd powinien dokładnie przeanalizować te raporty wydajności a kierownictwo IT powinno mieć możliwość wyjaśnienia odchyleń i problemów z wydajnością. Po weryfikacji powinny zostać rozpoczęte i kontrolowane odpowiednie działania w zakresie zarządzania

Ład informatyczny (IT governance) jest czymś innym niż zarządzanie IT (IT management). Ład określa, kto podejmuje decyzje. Zarządzanie to proces tworzenia i wdrażania decyzji [Weil, Ross 2004]. Ład informatyczny definiuje, kto jest uprawniony do podejmowania ważnych decyzji, kto ma głos i kto jest odpowiedzialny za realizację tych decyzji. To nie jest równoznaczne z zarządzaniem IT. Ład IT precyzuje uprawnienia decyzyjne, a zarządzanie IT przygotowuje i wdraża konkretne decyzje IT [Broadbent, 2003].

2. Modele ładu informatycznego

Wielu ekspertów zaleca szczegółowe modele realizowane przez kierowników średniego szczebla. Są one znane jako IT governance „frameworsks". Najczęściej stosowane modele to [Musson, 2009]:

– COBIT [COBIT, 2007],
– IT Infrastructure Library (ITIL) [OGC, 2009],
– ISO/IEC 27001 [ISO/IEC 27001, 2005].

Chociaż powyższe modele określane są jako "modele ładu informatycznego" część z nich w rzeczywistości jest modelami zarządzania [Bon, Jong, 2007]. Modele te nie są alternatywnymi sposobami postępowania z tymi samymi problemami.

COBIT jest modelem ładu informatycznego i wspierającym zestawem narzędzi, który umożliwia menedżerom na wypełnienie luki pomiędzy wymaganiami kontroli, kwestiami technicznymi i ryzykiem biznesowym. COBIT wymusza wyraźny rozwój polityk i dobrych praktyk kontroli IT w całej organizacji. COBIT podkreśla zgodność z przepisami, pomaga zwiększyć wartość osiąganą z IT, umożliwia dostosowanie i upraszcza wdrażanie modelu [COBIT, 2007].

ITIL jest w istocie szeregiem dokumentów, które są wykorzystywane, jako pomoc w implementacji modelu dla zarządzania usługami IT. Ten konfigurowalny model uściśla jak zarządzanie usługami winno być stosowane w organizacji. Chociaż ITIL został stworzony przez Centralną Agencji Informatyki i Telekomunikacji (Central Computer and Telecommunications Agency - CCTA), agencję rządową Wielkiej Brytanii, jest obecnie zaadoptowany i stosowany na całym świecie jako de facto standard w zakresie najlepszych praktyk w zakresie świadczenia usług IT. Chociaż ITIL obejmuje szereg obszarów, jego głównym celem jest na zarządzanie usługami IT [IT Service Management Zone, 2011].

ISO/IEC 27001:2005 jest standardem, który określa wymagania dla systemu zarządzania bezpieczeństwem informacji. Standard ten pomaga identyfikować, zarządzać i minimalizować zakres zagrożeń, którym informacje są regularnie poddawane. Norma ta została zaprojektowana, aby zapewnić dobór odpowiednich i proporcjonalnych do skali środków bezpieczeństwa, które będą chronić zasoby informacyjne i przez to wzbudzać zaufanie zainteresowanych stron [BSI Management Systems, 2011].

3. Standard ISO / IEC 38500:2008

Przykładem rosnącego znaczenia ładu IT jest wydany przez ISO światowy standard ISO, ISO / IEC 38500:2008 "Zasady ładu korporacyjnego technologii informatycznych", którego celem jest stworzenie ram zasad przeznaczonych do wykorzystania przez dyrektorów przy ocenie, kierowaniu i monitorowaniu wykorzystania IT w organizacji. Standard

ten uzupełnia zestaw norm ISO dotyczących systemów i technologii informacyjnych, tj. ISO/IEC 27000, ISO/IEC 20000, ISO/IEC 15504, ISO/IEC 24762, itd. Standard ten jest został przedstawiony Komisji Europejskiej 25 maja 2011.

Ten nowy standard wyznacza normy poprawnego stosowania procesów zarządzania i formułowania decyzji biznesowych w zakresie informacji i komunikacji, które są zwykle zarządzane przez wewnętrzne struktury lub dostawców usług zewnętrznych. W zasadzie wszystkie proponowane zasady zmierzają do trzech głównych celów:

- Zapewnienia zaangażowanych stron (menedżerów, konsultantów, inżynierów, producentów sprzętu, biegłych rewidentów, itp.), że, reguły ładu informatycznego są prawidłowo realizowane;
- Przekazywania informacji i wskazówek dla menedżerów dotyczących kontroli wykorzystania ICT w organizacji;
- Stanowienia podstawy do obiektywnej oceny przez kierownictwo wyższego szczebla zarządzania ICT.

ISO / IEC 38500:2008 został opublikowany w czerwcu 2008 roku na podstawie australijskiego standardu AS8015: 2005. Jest to pierwszy z serii zasad ładu IT. Ma on na celu stworzenie modelu zasad zarządzania organizacjami wykorzystywanego do oceny, zarządzania i monitorowania wykorzystania technologii informacyjnych (ICT). Norma ta jest zgodna z zasadami ładu korporacyjnego zawartymi w " Cadbury Report" i " Zasadami ładu korporacyjnego OECD ".

Normę tę stosuje się do procesów zarządzania ICT we wszystkich typach organizacji, które używają technologii informatycznych, dając podstawę do obiektywnej oceny wykorzystania ICT. Zarządzanie IT zgodne z normą obejmuje zgodność z:

- normami bezpieczeństwa,
- ochroną prywatności,
- ochroną przed spamem,
- właściwymi praktykami handlowymi,
- ochroną własności intelektualnej, w tym umów licencyjnych na oprogramowanie,
- przepisami dotyczącymi ochrony środowiska,
- zasadami bezpieczeństwa i higieny,
- prawami dostępu,
- normami odpowiedzialności społecznej.

Sprawność IT jest wyznaczana przez:

- prawidłowe wykorzystanie zasobów IT,

- określenie zakresu kompetencji i odpowiedzialności w osiąganiu celów organizacji,
- zapewnienie ciągłości i trwałości,
- dostosowanie technologii informacyjno-komunikacyjnych do potrzeb biznesowych,
- efektywną alokację zasobów,
- wprowadzanie innowacji w sektorze usług, rynków i przedsiębiorstw,
- stosowanie dobrych praktyk w relacjach z interesariuszami,
- redukcję kosztów,
- skuteczną materializację oczekiwane korzyści z każdej inwestycji w ICT.

W tym standardzie, ISO przytacza sześć zasad zarządzania IT [ISO/IEC 38500:2008, 2008]:

1. Odpowiedzialność – zarówno jednostki jak i grupy w organizacji muszą rozumieć i akceptować swoje obowiązki w zakresie podaży i popytu na IT. Osoby odpowiedzialne za działania mają prawo do realizacji tych działań. Biznes (klienci) i IT (dostawcy) powinni współpracować w duchu partnerstwa z wykorzystaniem efektywnej komunikacji bazując na pozytywnej i zaufanej relacji przy jasno określonym zakresie obowiązków i odpowiedzialności. Właściwie zarządzanie struktury organizacyjne, zadania i obowiązki muszą pozyskać mandat od władzy wykonawczej, zapewniający wyraźne uprawnienia i odpowiedzialności za ważne decyzje i zadania;
2. Strategia - strategia biznesowa organizacji bierze pod uwagę obecne i przyszłe możliwości IT. Plany strategiczne IT zaspokajają obecne i przewidywane potrzeby wynikające ze strategii organizacji. Planowanie strategiczne IT jest procesem złożonym i krytycznym dla przedsiębiorstwa. Wymaga ścisłej koordynacji między całym przedsiębiorstwem, jednostkami biznesowymi i planami strategicznymi. Cele wysokiego poziomu muszą zostać przekonwertowane na osiągalne plany taktyczne w celu zapewnienia minimalnego poziomu awarii i zaskoczeń. Planowanie strategiczne IT powinno zawierać przejrzyste i właściwe planowanie potencjału IT. Powinno ono obejmować ocenę zdolności obecnej infrastruktury IT i zasobów ludzkich niezbędnych do wsparcia przyszłych wymagań biznesowych i rozważania nowych osiągnięć technicznych, które mogłyby przyczynić się do przewagi konkurencyjnej i / lub optymalizacji kosztów. Zarządzanie zasobami IT wymaga powiązania z wieloma

zewnętrznymi dostawcami produktów i usług, którzy odgrywają kluczową rolę we wspieraniu biznesu. Strategiczne zarządzanie zaopatrzeniem zatem jest znaczącym punktem strategicznego planowania działalności wymagającym nadania kierunku i nadzoru;

3. Zakup – zakupy i przejęcia w IT są czynione z ważnych powodów, na podstawie odpowiednich i ciągłych analiz, skutkując jasnymi i przejrzystymi decyzjami. Istnieje równowaga pomiędzy korzyściami, możliwościami, kosztami i ryzykami, w perspektywie zarówno krótko-i długoterminowej. Przejęcia zasobów IT powinny być traktowane jako część głębszych zmian IT. Zdobyta technologia musi wspierać i działać w ramach istniejących i planowanych procesów biznesowych i infrastruktury IT. Wdrożenie zmian to nie tylko kwestia technologii, ale uwzględnienie zmian organizacyjnych, zmiany procesów biznesowych, przeprowadzenie szkoleń. Tworzone projekty powinny być analizowane w ramach szerszej skali całego przedsiębiorstwa, programów wpływających na inne projekty, tak aby stworzyć pełen zakres działań niezbędnych do zapewnienia sukcesu.
4. Wydajność - IT jest dostosowane do potrzeb w zakresie wspierania organizacji i świadczenia usług. Poziom usług i jakość usług muszą spełniać obecne i przyszłe wymagania biznesowe. Skuteczność pomiaru wydajności zależy od dwóch kluczowych aspektów: jasno określonych celów działania i ustanowienia skutecznych metryk monitorujących osiąganie celów. Proces pomiaru wydajności powinien być monitorowany konsekwentnie i rzetelnie;
5. Zasady zgodności - IT musi być zgodne z wszystkimi obowiązującymi przepisami i regulacjami. Polityki i praktyki muszą zostać jasno określone, wdrożone i egzekwowane. W dzisiejszym globalnym rynku, połączonym przez Internet pełnym zaawansowanych technologii, przedsiębiorstwa muszą spełniać coraz więcej wymogów prawnych i regulacyjnych. Istnieje rosnący wymóg, aby umowy IT zawierały ważne klauzule dotyczące prywatności, poufności, własności intelektualnej i bezpieczeństwa. Należy ustalić zasady i procedury dotyczące zarządzania i pracowników zapewniające, że cele przedsiębiorstwa są realizowane a ryzyko jest minimalizowane przy zachowanych zasadach zgodności;
6. Czynnik ludzki - zasady IT, praktyki i decyzje powinny głosić szacunek dla czynnika ludzkiego, dbając o istniejące i zmieniające się potrzeby wszystkich osób zaangażowanych w procesy. Realizacja

wszelkich projektów IT, w tym ład IT zazwyczaj wymaga znacznych zmian kulturowych i zmian zachowań w przedsiębiorstwie, jak również zmian współpracy z klientami i partnerami biznesowymi. Zarząd musi jasno precyzować cele, proponować szkolenia dla personelu oraz zwiększać umiejętności by być postrzeganym, jako pozytywnie wspierający proponowane zmiany.

ISO / IEC 38500 zaleca, aby firmy stosowały ład IT realizując trzy główne zadania:

- dokonanie oceny obecnego i przyszłego wykorzystania IT,
- szczegółowe przygotowanie i realizacja planów i polityk, które gwarantują, że korzystanie z IT spełnia cele biznesowe,
- kontrolowanie zgodności z politykami i wydajnością w stosunku do planów [ITGI, 2011].

4. Realizacja ładu IT

Przedsiębiorstwa realizują swoje rozwiązania w zakresie zarządzania poprzez szereg mechanizmów ładu tj.: struktury, procesy i komunikaty [Weil, Ross 2004]. Dobrze zaprojektowane, dobrze zrozumiane i przejrzyste mechanizmy ładu wspierają pożądane zachowania IT. Odwrotnie, jeśli mechanizmy są źle wdrażane, wtedy zasady ładu nie będą przynosiły pożądanych rezultatów.

Skuteczne zarządzanie wprowadza trzy rodzaje mechanizmów [ITGI, 2011]:

- Struktury podejmowania decyzji - jednostki organizacyjne i role odpowiedzialne za decyzje IT, takie jak komitety, zespoły wykonawcze i doradcy biznes / IT;
- Procesy dopasowania - formalne procesy zapewniające, że bieżące działania są zgodne z politykami IT i dostarczają informacji zwrotnych do decyzji. Zwierają one sugestie inwestycji IT i oceny procesów, procesy budowania wyjątków, umowy poziomu usług, obciążenia, i metryki;
- Procesy komunikacyjne - ogłoszenia, budowa kanałów informacyjnych oraz wysiłki edukacyjne, które rozpowszechniają zasady ładu IT, polityki i rezultaty procesów decyzyjnych IT.

Prezes Australijskiego Stowarzyszenia Informatycznego, Richard Hogg, powiedział: „Tak jak menedżerowie IT muszą poszerzyć swoje umiejętności, aby lepiej zrozumieć struktury i procesy biznesowe, które są zobowiązani wspierać, rady nadzorcze muszą nauczyć się, jakie pytania zadać na temat ładu IT (...) Złym jest ład korporacyjny, który spy-

cha ład IT w dół do poziomu zarządzania IT. ICT stanowi integralną część biznesu i ład IT jest integralną częścią ładu korporacyjnego [ASC, 2002]."

Zadawanie trudnych pytań jest skutecznym sposobem rozpoczęcia wdrożenia ładu IT. Oczywiście, osoby odpowiedzialne za ład chcą dobrych odpowiedzi na te pytania. Następnie chcą działania. Potem następuje faza obserwacji. Istotne jest, aby określić nie tylko działania, ale także kto jest odpowiedzialny za dostarczanie czego i w jakim czasie [ITGI, 2011].

Canadian Institute of Chartered Accountants (CICA) wydał broszurę o nazwie „20 pytań, które dyrektorzy powinni zadać na temat IT", aby pomóc dyrektorom korporacyjnym w wykonywaniu swoich obowiązków dotyczących IT. Dokument jest również pomocny dla audytu i komitetów sterujących IT [CICA, 2004]. Z analizy pytań jasno wynika, że główna odpowiedzialność spoczywa na zarządzaniu, które powinno wprowadzić niezbędne procedury. Członkowie zarządu powinni ustalić, czy zarząd sprawił, że owe procedury funkcjonują [ITGI, 2011].

Ponadto, jeżeli dyrektorzy mają przeprowadzić skuteczną rolę nadzoru w zakresie zarządzania IT, istnieje domniemanie, że będą oni niedbale podchodzili do tej funkcji, niezależnie od stopnia uczciwości i wiarygodności zarządzania. Dlatego niezbędne są pewne dowody potwierdzające. Dyrektorzy muszą określić, że procedury są na miejscu, że procedury są właściwe, i muszą uzyskać potwierdzające na to dowody [Trites, 2004].

Zakończenie

Dojrzałość zarządzania kluczowymi aktywami obecnie różni się znacząco w większości przedsiębiorstw. Finansowe i rzeczowe aktywa są zazwyczaj najlepiej zarządzane, a zasoby informacyjne są jednymi z najgorzej zarządzanych. Jednakże, ład IT powinien być integralną częścią ładu korporacyjnego. Zadawanie poprawnych pytań jest skutecznym sposobem, aby rozpocząć wdrażanie ładu IT. Członkowie zarządu muszą się nauczyć, jakie pytania zadać na temat ładu IT. Następnie, muszą otrzymywać dobre odpowiedzi na te pytania, które zmuszą ich do działań. Kolejnym krokiem jest wdrożenie systemu ładu IT poprzez zestaw mechanizmów ładu - struktur, procesów i komunikacji.

Literatura

1. IECD (2004), *Organisation for Economic Co-operation and Development, OECD Principles of Corporate Governance*, Francja, (także www.oecd.org/dataoecd/32/18/31557724.pdf).
2. Rock R., M. Otero, S. Saltzman (1998), *Principles and Practices of Microfinance Governance*, ACCION International, USA, wrzesień 1998 (także http://www.gdrc.org/icm/govern/govern.pdf).
3. Van Grembergen W., S. DeHaes (2008), *Implementing Information Technology Governance: Models, Practices and Cases*, IGI Publishing, USA.
4. Nolan R., F. W. McFarlen (2005), *Information Technology and the Board of Directors,* Harvard Business Review.
5. BIS, (1999), Bank for International Settlements, *Enhancing Corporate Governance in Banking Organisations, (*także www.bis.org/publ/bcbs122.pdf).
6. ITGI (2011), *Information Risks: Whose Business Are They?*
7. ISO (2008), International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/ IEC 38500:2008, *Corporate governance of information technology*, www.iso.org/iso/catalogue_detail.htm?csnumber=51639.
8. ITGI (2003), *Board Briefing on IT Governance*, 2nd Edition, USA.
9. Weill P., J. Ross (2004), *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business Press, USA.
10. Broadbent M. (2003), *Understanding IT Governance,* CIO Kanada.
11. Musson D. (2009), *IT Governance: A Critical Review of the Literature," Information Technology Governance and Service Management: Frameworks and Adaptations*, Ed. Aileen Cater-Steel, Information Science Reference, USA.
12. ITGI (2012), *COBIT*, www.isaca.org/cobit.
13. Office of Government Commerce (2009), *IT Infrastructure Library (ITIL) V3*, UK.
14. ISO and IEC, ISO/IEC 27001 (2005), *Information technology— Security techniques—Information security management systems—Requirements*, www.iso.org/iso/catalogue_detail?csnumber=42103.
15. Van Bon J., A. de Jong, A. Kolthof (2007), M. Pieper, R. Tjassing, A. van der Veen, T. Verheijen; *Foundations of IT Service Management Based on ITIL® V3*, Van Haren Publishing, Holandia.
16. Woźniak M. (2012), *Budowa zaufania w gospodarce elektronicznej przez zastosowanie użyteczności technologii i bezpieczeństwa witryny e-*

commerce, Zeszyty Naukowe Uniwersytetu Gdańskiego, Zarządzanie i Finanse Journal of Management and Finance, 2/1 2012.
17. IT Service Management Zone (2011), www.itil.org.uk.
18. BSI Management Systems (2011), www.bsi-emea.com.
19. ISO (2008), ISO/IEC 38500:2008.
20. ACS (2002), Australian Computer Society, *ACS Stresses Need for Better ICT Governance*.
21. ITGI (2011), *IT Governance Implementation Guide 2nd Edition*.
22. Canadian Institute of Chartered Accountants (CICA), (2004), *20 Questions Directors Should Ask About IT*, Kanada.
23. Trites, G. (2004), *Director Responsibility for IT Governance,* International Journal of Accounting Information Systems, vol. 5, issue 2.
24. ITGI (2011), IT Alignment: Who is in Charge?, 2011.
25. ITGI (2011), *Optimizing Value Creation From IT Investments*.
26. ITGI (2011), *Measuring and Demonstrating the Value of IT*.

Streszczenie

Funkcjonowanie efektywnego systemu ładu korporacyjnego w przedsiębiorstwie jak i w całej gospodarce pomaga osiągnąć taki poziom zaufania, jaki jest niezbędny do funkcjonowania gospodarki rynkowej. Ład korporacyjny jest procesem, w którym rada nadzorcza, poprzez kierownictwo, wspomaga instytucję w wypełnianiu misji i ochronie majątku. Efektywny ład korporacyjny ma miejsce, gdy zarząd przekazuje odpowiednie wskazówki dla kierownictwa zawierające strategiczne kierunki instytucji i nadzoruje wysiłki kierownictwa dążenia w tym kierunku. W ostatnich latach technologie informatyczne stały się szkieletem przedsiębiorstw. Dla wielu z nich byłoby niemożliwym funkcjonowanie bez IT. Technologie informatyczne nie są obecnie odseparowane od przedsiębiorstwa, są jego istotnym elementem. Kadra kierownicza w niedalekiej przeszłości mogła delegować, ignorować lub unikać decyzji związanych z IT. Obecnie w większości firm jest to niemożliwe. Brak nadzoru zarządu nad działaniami IT jest niebezpieczne; naraża przedsiębiorstwo na ryzyko w ten sam sposób, jak brak badania ksiąg rachunkowych. Bezwzględne uzależnienie od technologii informacyjnych zmusza do szczególnej koncentracji na ładzie informatycznym (IT governance) w celu zapewnienia, że inwestycje w IT wygenerują żądaną wartość biznesową a ryzyka związane z IT zostaną zminimalizowane. Głównym celem tego artykułu jest prezentacja kluczowych pojęć ładu informatycznego, opis najważniejszych modeli (frameworks) ładu informatycznego stosowanych przez organizacje, a także sprecyzowanie wytycznych dla organizacji w celu skutecznego, efektywnego i zyskownego wykorzystania IT bazując o normę ISO / IEC 38500:2008.

Słowa kluczowe
ład informatyczny, zarządzanie IT, ISO/IEC 38500

IT Governance based on ISO / IEC 38500 (summary)

The functioning of an effective system of corporate governance in the enterprise and across the economy helps to achieve this level of confidence that is necessary for the functioning of a market economy. Corporate governance is a process in which the board of directors, through management, supports the institution in fulfilling the mission and protect property. Effective governance occurs when the Board shall provide guidance for management institutions, including strategic direction and oversees the efforts of management efforts in this direction. In recent years, information technology became the backbone of business. For many of them would be impossible to function without IT. Information technologies are not currently separated from the company are its important element. Executives in the recent past could delegate, ignore or avoid decisions related to IT. Currently, most companies this is impossible. Lack of management oversight over the activities of IT is a dangerous, puts the company at risk in the same way as the lack of research accounts. The absolute dependence on information technology makes to the particular focus on IT governance to ensure that IT investments generate the desired business value and risk associated with IT is minimized. The main purpose of this article is to present the key concepts of IT Governance, a description of the major models (frameworks) IT governance used organizations, as well as to clarify guidelines for the organization for the effective, efficient and profitable use of IT based on standard ISO / IEC 38500:2008. This article should help the board members to implement IT governance.

Keywords
IT Governance, IT management, ISO / IEC 38500