Czym jest, a czym nie defraudacja

NA POCZĄTEK WARTO ZADAĆ PYTANIE I UŚCIŚLIĆ, CZYM TAK NAPRAWDĘ JEST DEFRAUDACJA, I JAK TO POJĘCIE MA SIĘ DO ROZPOZNAWALNEJ PRZEZ KAŻDEGO KRADZIEŻY. O TYM, ŻE NIE JEST ONO KRADZIEŻY DALEKIE I NOSI JEJ PODSTAWOWE ZNAMIONA, ŚWIADCZY FAKT, IŻ POTOCZNIE DEFRAUDACJĘ OKREŚLA SIĘ „KRADZIEŻĄ W BIAŁYCH RĘKAWICZKACH".

W literaturze polskiej defraudacja zastępowana jest często pojęciem nadużycia. Termin ten właściwie oddaje to, czym defraudacja jest, czyli wykorzystywaniem pozycji zawodowej w ramach zatrudnienia w przedsiębiorstwie do osiągania prywatnych korzyści materialnych.

Zwykle z korzyściami prywatnymi związane są analogiczne lub większe straty przedsiębiorstwa, w którym defraudacja ma miejsce. Większe straty po stronie przedsiębiorstwa wynikają z kosztów, jakie jednostka musi ponieść po odkryciu defraudacji, a które związane są z koniecznością uporządkowania bałaganu organizacyjnego powstałego na skutek procesów defraudacyjnych oraz przywracania utraconej wiarygodności w oczach kontrahentów, pracowników i całej reszty otoczenia przedsiębiorstwa. Warto pamiętać, że utrata wiarygodności może następować także jeszcze przed całkowitym ujawnieniem defraudacji, kiedy część kontrahentów, obserwując nietypowe praktyki stosowane przez przedsiębiorstwo, domyśla się, że ma do czynienia z jednostką „zarażoną" defraudacją i, tracąc do takiej jednostki zaufanie, stopniowo redukuje swoją kooperację, ostrzegając przy tym inne firmy zaprzyjaźnione. Tym samym jednostka ponosi trudne do oszacowania, duże koszty i traci wiele korzyści.

Defraudacja polega na dokonywaniu błędów świadomych, które mogą też przybrać formę świadomych przeoczeń i zaniechań, którymi może być zainteresowana chociażby konkurencja jednostki. Nie uważa się za defraudację błędów i zaniechań nieświadomych, powstałych na skutek niedopatrzeń lub braku dochowania należytej staranności. W praktyce trudno jednoznacznie zweryfikować intencjonalność popełnienia błędu. Dlatego też, aby ocenić, co jest, a co nie jest defraudacją najłatwiej zweryfikować, czy popełnione błędy przyczyniły się do uzyskania korzyści osoby lub grupy, która je popełniła lub za nie odpowiada.

DEFRAUDACJA WSPÓŁCZESNA

Defraudacja współcześnie spotykana, podobnie jak cała otaczająca nas rzeczywistość, ma charakter zdecydowanie bardziej wirtualny i jest bardziej wyrafinowana w swoich technikach niż ta tradycyjna, z którą zmagało się poprzednie pokolenie. Współczesne techniki nadużyć często bazują na znajomości systemów informatycznych i umiejętności wykorzystywania ich nieszczelności w praktyce. Zależność współczesnych organizacji od narzędzi informatycznych jest ogromna i cały czas rośnie. Warto pamiętać, że z tą zależnością i wszechobecnością systemów informatycznych rosną także możliwości dokonywania coraz bardziej wyrafinowanych w formie i coraz trudniejszych do identyfikacji fałszerstw. Oczywiście trudno zaprzeczyć, że właściwie zaprojektowane systemy finansowo-księgowe i controllingowe mogą także pomóc w wykrywaniu i wczesnym przeciwdziałaniu defraudacjom. Aby tak się stało, konieczna jest jednak identyfikacja kluczowych elementów ryzyka i możliwości dokonywania nadużyć oraz opracowanie i wdrożenie kontroli wewnętrznych,

DEFRAUDACJA POLEGA NA DOKONYWANIU BŁĘDÓW ŚWIADOMYCH, KTÓRE MOGĄ TEŻ PRZYBRAĆ FORMĘ ŚWIADOMYCH PRZEOCZEŃ I ZANIECHAŃ.

które tym elementom ryzyka będą zapobiegać. Niestety stosunkowo często brak jest pełnej świadomości ryzyka defraudacji, w szczególności tych jego czynników, które są konsekwencją luk w systemach finansowo-księgowych i controllingowych. Dotyczy to także większych i dojrzalszych organizacji. Wydaje się, że taki stan rzeczy w wielu przypadkach może mieć swoje źródło w nadmiernym zaufaniu do systemów i do nieomylności „automatów" w nich działających. Zapomina się jednak, że najczęściej wykorzystywane przez jednostki systemy informatyczne w zakresie transakcyjnym, finansowo-księgowym czy też controllingowym są wystandaryzowane. Takie systemy, bez odpowiedniego zaprojektowania, dostosowania ich do organizacji czy też wprowadzenia odpowiadających strukturze organizacyjnej podziałów obowiązków oraz kompetencji kontroli dostępowych, nie będą działać i chronić właściwie. Aby do tego nie dopuścić, należy wespół z konsultantami wdrażającymi system dokonać analizy ryzyka defraudacji, w szczególności tych przypadków, które mogą zostać dokonane przy wykorzystaniu systemu i rozważyć, czy i w jaki sposób im przeciwdziałać, oraz – na koniec – opracować i wdrożyć środki zapobiegawcze. Nie zawsze organizacja posiada wystarczające kompetencje, żeby właściwie określić czynniki ryzyka defraudacji i zaprojektować optymalne kontrole im przeciwdziałające. W takich wypadkach warto rozważyć skorzystanie z pomocy konsultantów zewnętrznych, którzy, wykorzystując swoje doświadczenia w podobnych projektach wykonanych dla innych organizacji, umożliwią przejście przez proces projektowania i wdrożenia kontroli antydefraudacyjnych w sposób sprawny, skuteczny i przewidywalny.

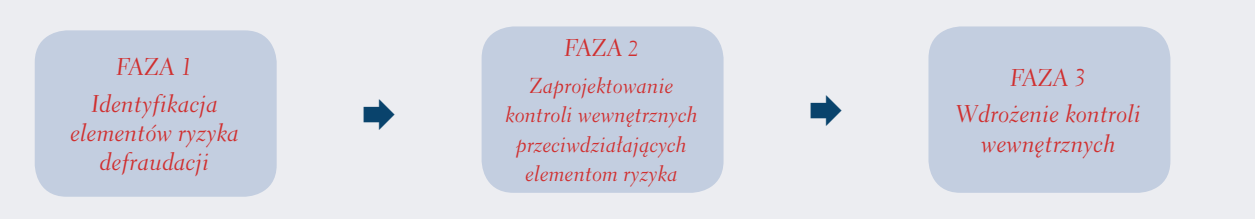
Na defraudacje o współczesnym charakterze najbardziej narażone są przedsiębiorstwa z dużą liczbą transakcji jednorodnych, posiadające skomplikowane, rozbudowane, często nieprzejrzyste struktury organizacyjne i niespójne, nakładające się kompetencje w ramach podziału obowiązków. Za postępującym stopniem skomplikowania i wielorakich, przenikających się współzależności często idzie stopień informatyzacji i zależności od systemów. Branże, w których należy szukać jednostek szczególnie narażonych na nadużycia to: handel detaliczny (sieci sklepów detalicznych, ale także sieci super- i hipermarketów), transport, logistyka i spedycja czy też wszelkiego typu usługi masowe, takie jak: usługi płatnych telewizji i Internetu, telekomunikacja, turystyka oraz sieci restauracji i kawiarni.

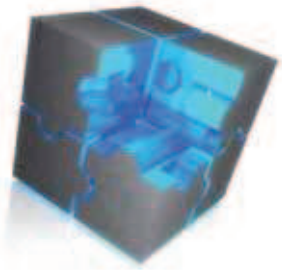
PODSTAWOWE CZYNNIKI RYZYKA I PRZYPADKI DEFRAUDACJI

Typowe czynniki ryzyka i przypadki nadużyć spotykane współcześnie w przedsiębiorstwach to:

- zakupy po zawyżonych cenach – zakup odbywa się po cenie wyższej niż regularna cena rynkowa; różnica na pojedynczej sztuce nie jest znaczna, natomiast przy dużym obrocie generuje dodatkowy zysk, który stanowi korzyść dla osób uczestniczących w defraudacji;
- sprzedaż po zaniżonych cenach – działa podobnie jak zakup po zawyżonych cenach; tym razem sprzedaż odbywa się po cenach niższych niż regularnie stosowane a nieautoryzowany „rabat" przy dużej ilości stanowi źródło korzyści wynikających z nadużycia;

DIAGRAM 1. SYSTEM PRZECIWDZIAŁANIA DEFRAUDACJI *Źródło: opracowanie własne*





ZALEŻNOŚĆ WSPÓŁCZESNYCH ORGANIZACJI OD NARZĘDZI INFORMATYCZNYCH JEST OGROMNA I CAŁY CZAS NIEUCHRONNIE ROŚNIE.

- oszustwa w przelewach/płatnościach bankowych, które zmierzają do wykonania płatności na prywatny rachunek osoby dokonującej defraudacji lub osoby jej bliskiej – odbywają się najczęściej poprzez zmianę danych przelewu w części dotyczącej numeru rachunku czy też dokonywaniu przelewów na niewielkie kwoty, poniżej progu kontroli wewnętrznej; aby ukryć fałszerstwo, takie fikcyjne płatności są kolejno ujmowane jako rozrachunki nierozliczone i spisywane w koszty działalności operacyjnej; czasami oszustwa dotyczące rachunków bankowych mogą polegać na blokowaniu środków pieniężnych firmy na własnym koncie i inwestowaniu ich przejściowo w ciągu miesiąca na własny rachunek; takie sytuacje narażają spółki na szczególnie wysokie straty wówczas, kiedy inwestycje dotyczą instrumentów ryzykownych o dużej zmienności cen, tj. instrumenty pochodne lub akcje;
- sprzedaż towaru/usługi poza przedsiębiorstwem (w całości lub w części) – sprzedaż towaru lub usługi firmy odbywa się w całości lub części poza przedsiębiorstwem i często bez wystawienia dodatkowej faktury sprzedaży; te nadużycia w praktyce są popełniane przez osoby obsługujące magazyn i posiadające dostęp oraz możliwość nieautoryzowanego wydania towaru z magazynu lub w firmach usługowych przez osoby z działów realizacji i sprzedaży usług;
- fikcyjne rozrachunki/fikcyjny kontrahent – faktura zakupu od fikcyjnego kontrahenta i za fikcyjny zakup jest księgowana oraz regulowana na rachunek prywatny; nadużycie jest szczególnie łatwe do przeprowadzania przez działy księgowości firm, gdzie funkcje księgowania faktur zakupu i możliwości dokonywania przelewów bankowych nie są rozdzielone;
- manipulacje wynikiem finansowym – najczęściej manipulacje odbywają się poprzez przyspieszone fakturowanie, bez wydania towaru lub z wydaniem mającym znamiona fikcyjnego (po końcu roku nastąpi zwrot); w przedsiębiorstwach usługowych nadużycie przybiera formę manipulowania momentem powstania przychodu i polega na wykazywaniu wyższego stopnia realizacji kontraktów długoterminowych lub rozpoznawaniu przychodów z usług, które nie zostały jeszcze faktycznie zrealizowane lub zrealizowano je już w nowym okresie sprawozdawczym; manipulacje zmierzają najczęściej do wykazania wyniku finansowego lepszego niż faktycznie uzyskany i mogą mieć na celu otrzymanie bonusów przez sprzedawców, działy realizacji usług lub zarząd, czy też wypełnienie oczekiwań finansujących (banki, fundusze) i akcjonariuszy; powstawanie tego typu nadużyć jest udziałem jego podstawowych beneficjentów, tj. sprzedawców, kierowników działów realizacji i w szczególności zarządu;
- sprzedaż powyżej limitu kredytowego – sprzedaż odbywa się pomimo przekroczenia limitu kredytowego; istnieje ryzyko braku płatności z uwagi na niewypłacalność kontrahenta; często w tych przypadkach osoba dokonująca sprzedaży uzyskuje korzyść w postaci tzw. łapówki.

Obok ww. rozwijają się formy bardziej tradycyjne, które z biegiem czasu przenikają się ze współczesnymi i przyjmują bardziej wyrafinowane postaci. W taki sposób:

- klasyczna kradzież z magazynu obecnie często łączy się ze sprzedażą na własny rachunek i przybiera formę sprzedaży bez faktury, także skierowanej do nieuczciwych klientów przedsiębiorstwa;
- klasyczna kradzież środków pieniężnych z kasy – ponieważ w większości firm obrót środkami pieniężnymi w kasie został w ciągu ostatnich lat ograniczony, nadużycie obecnie zastąpione zostało opisanymi powyżej fałszerstwami dokonywanymi poprzez wykorzystywanie dostępu do transakcji na rachunkach bankowych;
- fikcyjne rachunki na potrzeby prywatne, tj. taxi, hotele, konsumpcja – tradycyjnie nadużycie dokonywane najczęściej w związku z rozliczaniem wydatków służbowych zmierzało do zakupów za środki spółki na prywatne potrzeby; współcześnie wciąż aktualne; przyjmuje także formę nieautoryzowanych, często niepotrzebnych lub nadmiernych zakupów towarów lub usług za dodatkową korzyść w postaci łapówki.

Analizując wymienione powyżej elementy ryzyka i przypadki defraudacji, widać wyraźnie, że działy najbardziej narażone na powstawanie nadużyć to: Dział Sprzedaży, Dział Zakupów oraz Księgowość. Na szczególne podkreślenie w tym wypadku zasługuje Zarząd, który – jako ścisłe kierownictwo jednostki – posiada szerokie możliwości pomijania

TABELA 1. RYZYKA DEFRAUDACJI I PRZYKŁADOWE KONTROLE IM PRZECIWDZIAŁAJĄCE *Źródło: opracowanie własne*

Typowe ryzyka defraudacji	Obszar powstawania	Przykładowa kontrola przeciwdziałająca
Zakup po zawyżonych cenach	Zakupy	Ustalone ceny zakupu na standardowe towary/materiały/ /usługi (wprowadzenie benchmarku ceny oraz granic rozbieżności); automatyczny systemowy raport rozbieżności powyżej oczekiwań
Sprzedaż po zaniżonych cenach	Sprzedaż	Ustalone ceny sprzedaży – kontrola poprzez system; brak możliwości zmiany ceny lub udzielenia rabatu przy wystawianiu faktury poza określonym przedziałem %; w przypadku zmiany powyżej przedziału konieczna akceptacja elektroniczna przełożonego
Oszustwa w płatnościach/ /przelewach bankowych (np. płatność na rachunek prywatny, podwójna płatność)	Księgowość/Treasury	Automatyczny raport wyjątków na poziomie systemu transakcyjnego banku (w ramach raportu wyjątków: weryfikacja płatności na tę samą kwotę na dwa różne rachunki, weryfikacja płatności na nieautoryzowane numery rachunków bankowych)
Sprzedaż towaru/usługi poza przedsiębiorstwem (w całości lub w części)	Sprzedaż/Księgowość	Nieautoryzowana sprzedaż towaru/usługi – podział obowiązków: oddzielenie wystawiania faktury od wydania z magazynu/wykonania usługi; nieautoryzowane wydanie z magazynu – regularne wyrywkowe inwentaryzacje
Fikcyjne rozrachunki Fikcyjny kontrahent	Księgowość/Zakup	Niezależna od Działu Zakupów weryfikacja danych kontrahentów po wprowadzeniu do systemu. Automatyczna kontrola systemowa dostępu do wprowadzania danych kontrahentów (dostęp systemowy wyłącznie dla osób upoważnionych); faktury od „przypadkowych" kontrahentów weryfikowane wyrywkowo niezależnie
Podwójna faktura zakupu	Księgowość/Zakup	Elektroniczny system akceptacji faktur zakupu; brak księgowania faktury bez akceptacji; przy akceptacji systemowe „łączenie" z zamówieniem
Fikcyjne rachunki (taxi, hotele, konsumpcja)	Księgowość/Administracja/ /Zakupy	Akceptacja rachunków przez przełożonego; dla skutecznej weryfikacji kompletności wprowadzenie elektronicznego obiegu dokumentów; przypisanie kosztów w trakcie akceptacji do kontraktów/zleceń wykonywanych
Manipulacje wynikiem finansowym przez sprzedawców (przyspieszone fakturowanie, manipulowanie momentem powstania przychodu)	Sprzedaż/ Księgowość	Podział obowiązków: oddzielenie wystawiania faktur od wykonywania usług/wydawania towarów z magazynu; niezależna od Działu Sprzedaży i Realizacji weryfikacja stopnia realizacji kontraktów długoterminowych
Nieautoryzowane zakupy towarów/usług	Zakup/Księgowość	Akceptacja rachunków przez przełożonych osób dokonujących zakupy; dla skutecznej weryfikacji kompletności warto wprowadzić elektroniczny obieg dokumentów oraz bieżące przypisywanie kosztów w trakcie akceptacji do kontraktów/zleceń wykonywanych
Sprzedaż powyżej limitu kredytowego/do kontrahenta niewypłacalnego	Sprzedaż	Weryfikacja limitu kredytowego poprzez system; brak możliwości dokonania sprzedaży (wystawienia faktury sprzedaży, dokumentu wydania z magazynu) po przekroczeniu limitu kredytowego bez dodatkowej akceptacji przełożonego

SYSTEMY FINANSOWO-KSIĘGOWE I CONTROLLINGOWE MOGĄ ISTOTNIE POMÓC W PRZECIWDZIAŁANIU DEFRAUDACJOM.

wszelkich kontroli wewnętrznych i praktycznie nieograniczony „potencjał" dokonywania nadużyć. Pomocnym w zmniejszaniu tego „potencjału" może okazać się odpowiedni podział obowiązków oraz struktura i kultura organizacyjna, która nie pozwala na zupełnie samodzielne, bez niczyjej wiedzy, działania Zarządu. Aby ograniczyć możliwości nadużyć i niekontrolowanych działań Zarządu, akcjonariusze dużych jednostek, w szczególności tych o publicznym charakterze czy też publicznego zainteresowania, wprowadzają dodatkowy organ nadzoru właścicielskiego w postaci rady nadzorczej, i raportującego do nich bezpośrednio audytu wewnętrznego.

JAK ZAPOBIEGAĆ? CZY I JAK SYSTEM CONTROLLINGOWY MOŻE POMÓC?

Metodologia tworzenia systemów przeciwdziałania defraudacjom jest zbieżna z innymi metodologiami stosowanymi przy opracowywaniu systemów kontroli wewnętrznych i zawiera się w trzech podstawowych fazach:

1. Identyfikacja elementów ryzyka defraudacji.
2. Zaprojektowanie kontroli wewnętrznych przeciwdziałających elementom ryzyka (należy pamiętać, że kontrole wewnętrzne obejmują w tym wypadku także kontrole zautomatyzowane, dokonywane przy użyciu systemów finansowo-księgowych i controllingowych).
3. Wdrożenie kontroli wewnętrznych.

Zamieszczona poniżej tabela podsumowuje przedstawione w artykule rozważania dotyczące typowych czynników ryzyka i przypadków defraudacji, na które narażone są współcześnie funkcjonujące organizacje. Podanie w tabeli przykładowych kontroli przeciwdziałających opisanym wcześniej częstym przypadkom defraudacji ma na celu pomoc i zainspirowanie przy projektowaniu systemów kontroli wewnętrznych zapobiegających lub minimalizujących ryzyko powstawania nadużyć. Z analizy tabeli wynika, że większość kontroli przeciwdziałających defraudacjom może następować w znacznej części automatycznie przy użyciu systemów dostępnych w jednostce. Dowodzi to, iż systemy finansowo-księgowe i controllingowe mogą istotnie pomóc w przeciwdziałaniu defraudacjom. Współczesne narzędzia informatyczne o charakterze controllingowo-finansowo-księgowym oferują bowiem szerokie możliwości w zakresie zaawansowanej analizy danych czy też identyfikacji i śledzenia transakcji o znamionach defraudacji. Szybkie i skuteczne wykrywanie i często wczesne uniemożliwianie rozprzestrzeniania się defraudacji jest możliwe szczególnie poprzez zautomatyzowane raporty wyjątków, wskazujące na podejrzane operacje.

Nie należy jednakże zapominać, iż zanim wspomniane kontrole automatyczne zaczną działać samoczynnie, niezbędny jest odpowiedni udział czynnika ludzkiego. Udział ten często dotyczy wprowadzania danych do systemu oraz weryfikacji tych danych. Dla pełnej skuteczności kontroli zautomatyzowanych konieczne staje się zapewnienie niezależności wprowadzania i weryfikacji tych danych od osób i działów, które będą kontrolowane. Istotna jest tutaj szczelność dostępu do wprowadzania i zmiany danych, polegająca na ograniczeniu dostępu wyłącznie do niezależnych osób upoważnionych.

Często jednostki czy ich kierownictwa brak ryzyk defraudacji tłumaczą istnieniem kultur organizacyjnych wprowadzanych mniej lub bardziej sformalizowanymi regulaminami, czy też kodeksami etycznymi. Warto zauważyć, że o ile wymienione elementy determinują środowisko kontroli wewnętrznej na najwyższym szczeblu, są jedynie warunkiem koniecznym, a nie wystarczającym zapewnieniem skutecznej ochrony przed defraudacjami w przedsiębiorstwie.

Przy projektowaniu systemów przeciwdziałania nadużyciom warto zdawać sobie sprawę z ograniczeń tych systemów. Wynikają one z braku możliwości stworzenia systemu, który byłby w stanie zaadresować wszystkie możliwe ryzyka nieodłącznie związane z defraudacją, takie jak chociażby udział kierownictwa najwyższego szczebla czy też zmowa osób z różnych działów. Optymalny system przeciwdziałania ryzyku defraudacji powinien zapewnić maksimum ochrony przed kluczowymi dla danej jednostki czynnikami ryzyka przy założonym koszcie. ■

GRZEGORZ BŁASZKOWSKI

Biegły rewident, członek ACCA. Przez ostatnie 10 lat związany z wiodącymi globalnymi firmami konsultingowymi: KPMG oraz Ernst & Young. Obecnie jako właściciel BŁASZKOWSKI ADVISORY SERVICES niezależnie zajmuje się badaniem sprawozdań finansowych oraz doradztwem finansowo-rachunkowym, m.in. w zakresie raportowania, systemów controllingowych i kontroli wewnętrznej, defraudacji oraz Komitetów Audytu.