Rola kontroli wewnętrznej i audytu wewnętrznego w wykrywaniu nadużyć pracowniczych – case studies

Marek Błażejewski

Manager BRS
Certified in Cybersecurity (CC)

Grant Thornton

Agenda

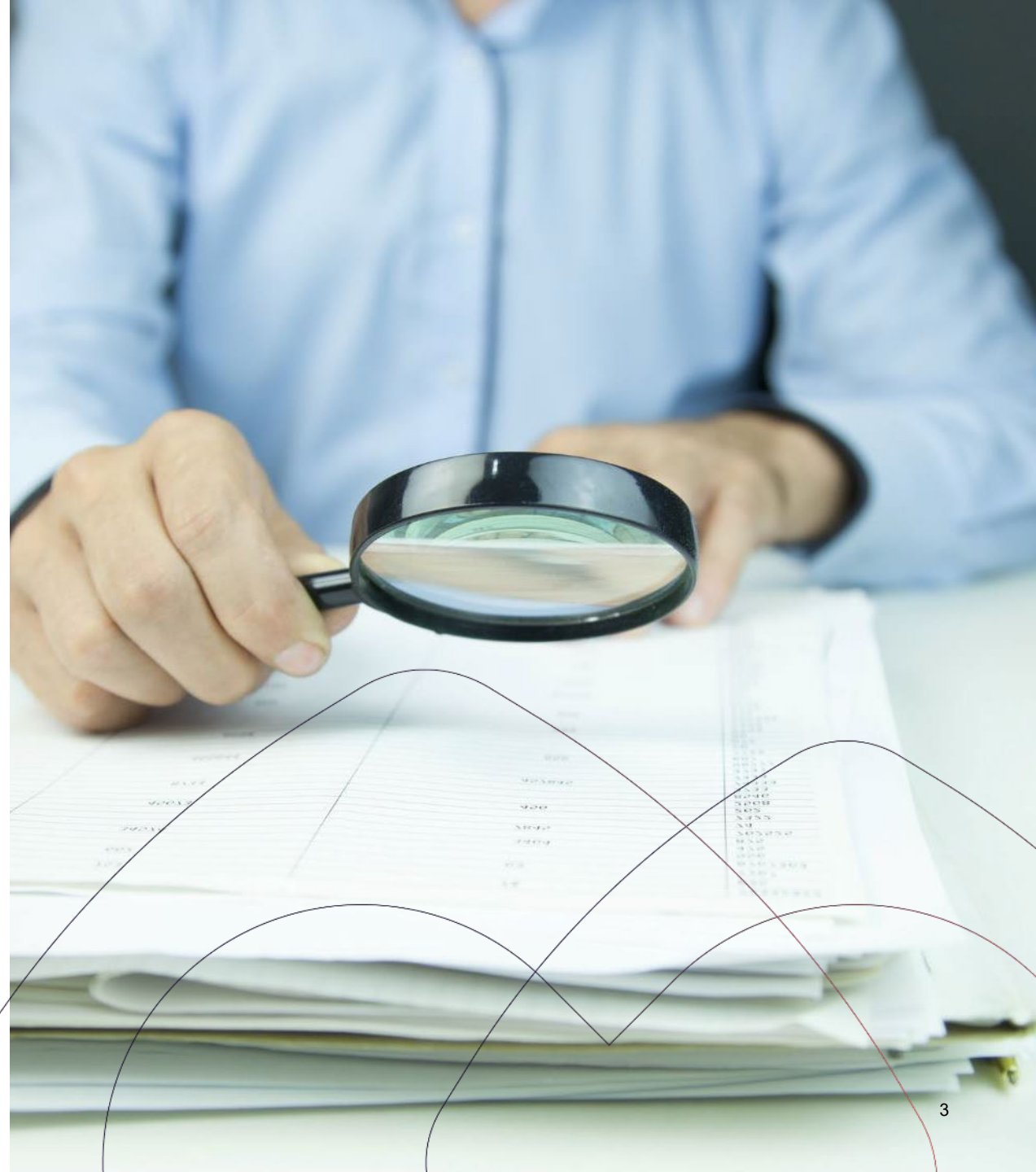
1. Jak definiujemy oszustwa i nadużycia pracownicze?
2. Rodzaje oszustw i nadużyć pracowniczych
3. Jak dochodzi do oszustw i nadużyć?
4. Jak zidentyfikować potencjalne oszustwa i nadużycia?
5. Oszustwa i nadużycia pracownicze w liczbach
6. Odpowiedzi na zidentyfikowane ryzyko oszustw i nadużyć
7. Studium przypadku
8. Podsumowanie

Jak definiujemy oszustwa i nadużycia pracownicze?

Oszustwo (ang. *fraud*) w potocznym i słownikowym rozumieniu definiowane jest jako świadome wprowadzenie kogoś w błąd lub wykorzystanie czyjegoś błędu dla własnej korzyści.

Nadużycie (też często tłumaczenie angielskiego słowa *fraud*) według Słownika Języka Polskiego PWN to postępowanie lub czyn niezgodne z przyjętymi normami postępowania.

Nadużycia pracownicze lub zawodowe (ang. *occupational fraud*) to nadużycia popełniane przez pojedyncze osoby lub niewielkie grupy osób w związku z ich zajęciem zawodowym. Pojęcie zajęcia zawodowego obejmuje w tym przypadku zarówno zatrudnienie (pracownik, urzędnik, zleceniobiorca, wykonawca), działalność gospodarczą (właściciel, wspólnik) jak i działalność w zawodzie zaufania społecznego.



Grant Thornton

Oszustwa i nadużycia według polskich przepisów karnych

- Przestępstwa przeciwko wiarygodności dokumentów (rozdział XXXIV KK), w tym m.in.
  - Fałszowanie dokumentów
  - Fałszowanie faktur
- Przestępstwa przeciwko mieniu (rozdział XXXV KK), w tym m.in.
  - Kradzież mienia (zabór cudzej rzeczy wbrew woli jej właściciela)
  - Przywłaszczenie mienia (legalnie powierzone mienie zostało np. sprzedane lub nie jest zwracane właścicielowi)
  - Oszustwo (doprowadzenie innej osoby do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania celem uzyskania własnej korzyści majątkowej)
  - Oszustwo komputerowe (nieupoważnione wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody)

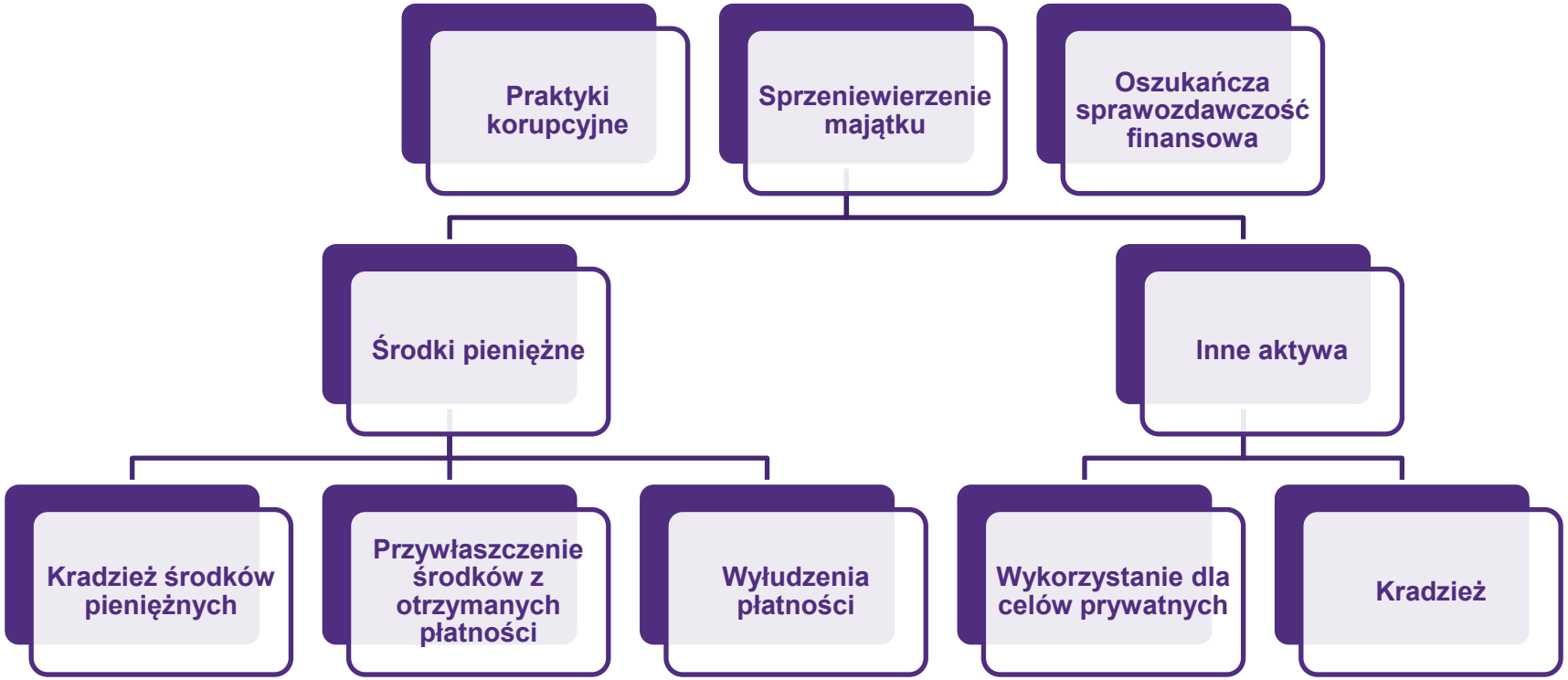
Oszustwa i nadużycia według polskich przepisów karnych (c.d.)

- **Przestępstwa przeciwko obrotowi gospodarczemu i interesom majątkowym w obrocie cywilnoprawnym (rozdział XXXVI KK), w tym m.in.**
  - Nadużycie zaufania
  - Łapownictwo menedżerskie
  - Oszustwo finansowe
  - Oszustwo ubezpieczeniowe
  - Pranie brudnych pieniędzy
  - Nieprowadzenie dokumentacji działalności gospodarczej albo prowadzenie jej w sposób nierzetelny lub niezgodny z prawdą
- **Przestępstwa przeciwko obrotowi pieniędzmi i papierami wartościowymi (rozdział XXXVII KK), w tym m.in.**
  - Oszustwo kapitałowe (rozpowszechnianie w dokumentacji związanej z obrotem papierami wartościowymi nieprawdziwych informacji lub przemilcza informacje o stanie majątkowym oferenta, mające istotne znaczenie dla nabycia, zbycia papierów wartościowych, podwyższenia albo obniżenia wkładu)
- **Przestępstwa przeciwko przepisom ustawy o rachunkowości (art. 77 – 79), w tym m.in.**
  - nieprowadzenie ksiąg rachunkowych, prowadzenia ich wbrew przepisom ustawy lub podawania w tych księgach nierzetelnych danych

Grant Thornton

Rodzaje oszustw i nadużyć pracowniczych

Stowarzyszenie Biegłych ds. Przestępstw i Nadużyć Gospodarczych (ACFE) klasyfikuje oszustwa i nadużycia pracownicze w sposób następujący:



Źródło: Occupational Fraud 2024: A Report to the Nations. Copyright 2024 by the Association of Certified Fraud Examiners, Inc.

Grant Thornton

Trójkąt oszustwa czyli jak dochodzi do nadużyć

Przyczyny występowania nadużyć i oszustw mogą być różnorodne, ale najczęściej pojawiają się, gdy zachodzą łącznie następujące okoliczności:

PRESJA

finansowe lub emocjonalne naciski, które skłaniają jednostki do popełniania oszustw. Może to obejmować czynniki takie jak trudności finansowe, uzależnienie lub pragnienie wyższego standardu życia.

RACJONALIZACJA

usprawiedliwienie swoich oszukańczych działań przed sobą samymi. Obejmuje ono tworzenie wymówek lub przekonywanie siebie, że oszustwo jest konieczne lub moralnie akceptowalne w konkretnej sytuacji.

OKAZJA

warunki lub sytuacje, które pozwalają na wystąpienie oszustwa. Obejmuje to słabe wewnętrzne kontrole organizacji, brak nadzoru lub pozycję zaufania i władzy, która może być wykorzystana.

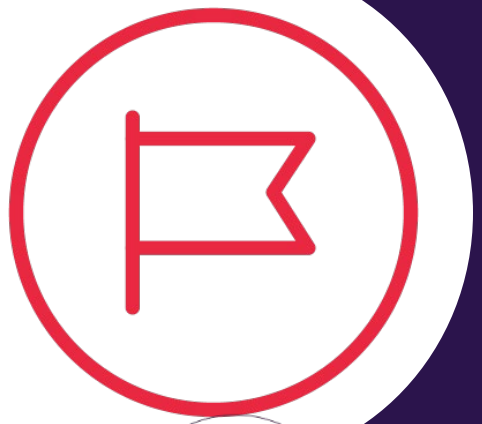
Źródło: opracowanie własne na podstawie Donald R. Cressey: Other People's Money (Montclair Nj: Patterson Smith, 1973)

Grant Thornton

Jak zidentyfikować potencjalne oszustwa i nadużycia?

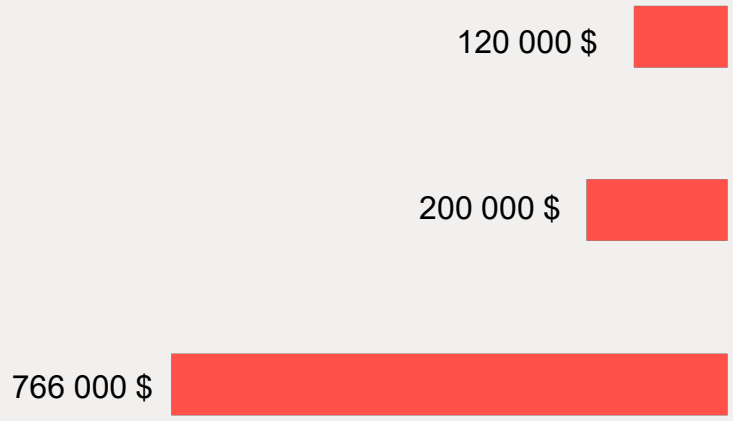
Identyfikacja potencjalnych oszustw i nadużyć nie jest prosta. Im więcej osób jest zaangażowanych w dany proceder, tym prawdopodobieństwo wykrycia jest niższe. Ważnym elementem przyczyniającym się do wykrywania jest identyfikacja tzw. czerwonych flag, np.:

- Życie ponad stan
- Trudności finansowe danego pracownika
- Niezwykle bliskie powiązanie z dostawcą/klientem
- Zidentyfikowane uchybienia w czynnościach kontrolnych, niechęć do dzielenia się obowiązkami
- Postawa pracownika wyrażająca się w drażliwości, podejrzliwość lub postawie obronnej
- Znęcanie się lub zastraszanie
- Rozwód/problemy rodzinne
- Postawa „na cwaniaka/kombinatora”
- Nadmierna presja ze strony organizacji
- Problemy z uzależnieniem
- Skargi na nieodpowiednie wynagrodzenie
- Niechęć do korzystania z urlopów
- Izolacja społeczna
- Wcześniejsze problemy z prawem
- Nadmierna presja rodziny/rówieśników na sukces

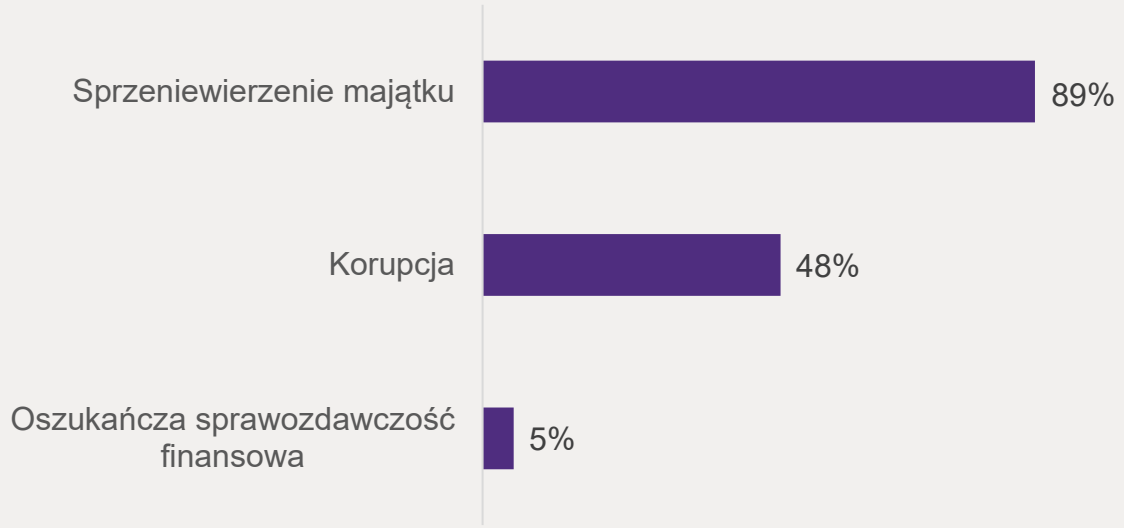


Oszustwa i nadużycia w liczbach

Raz na 2 lata Stowarzyszenie Biegłych ds. Przestępstw i Nadużyć Gospodarczych (ACFE) przygotowuje Raport do Narodów przedstawiający oszustwa i nadużycia pracownicze na świecie.



mediana straty



udział przypadków

Źródło: Occupational Fraud 2024: A Report to the Nations. Copyright 2024 by the Association of Certified Fraud Examiners, Inc.

Oszustwa i nadużycia w liczbach

W których departamentach jednostek oszustwa i nadużycia są identyfikowane najczęściej?

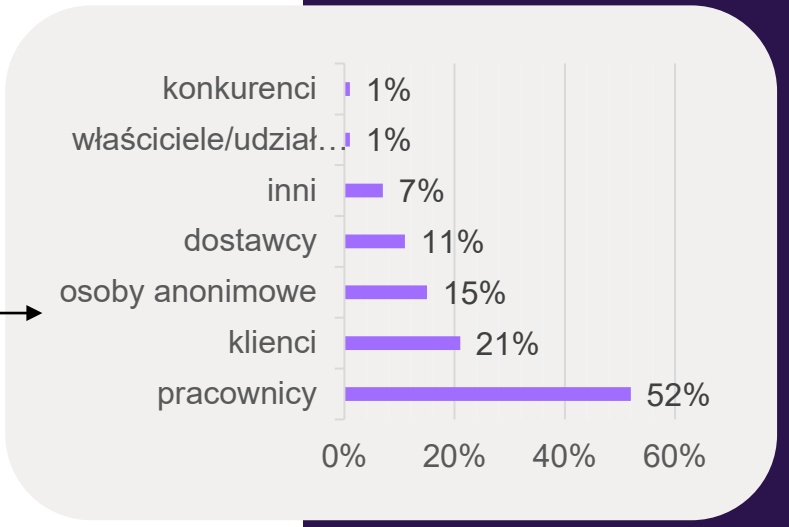
Dział	udział	mediana straty
Operacyjny	14%	$100 000
Księgowość	12%	$208 000
Sprzedaż	12%	$55 000
Kierownictwo/wyższy menedżement	9%	$75 000
Customer service	9%	$793 000
Zakupy	7%	$143 000
Wsparcie administracyjne	6%	$88 000
Finanse	5%	$285 000
Magazyny/zapasy	4%	$156 000
Inwestycje/utrzymanie ruchu	4%	$800 000
Produkcja	3%	$200 000
IT	3%	$120 000
Zarząd	2%	$150 000
HR	2%	$321 000
Marketing/public relations	1%	$100 000
R&D	1%	*

Źródło: Occupational Fraud 2024: A Report to the Nations. Copyright 2024 by the Association of Certified Fraud Examiners, Inc.

Grant Thornton

Oszustwa i nadużycia w liczbach

Jak oszustwa i nadużycia są identyfikowane?

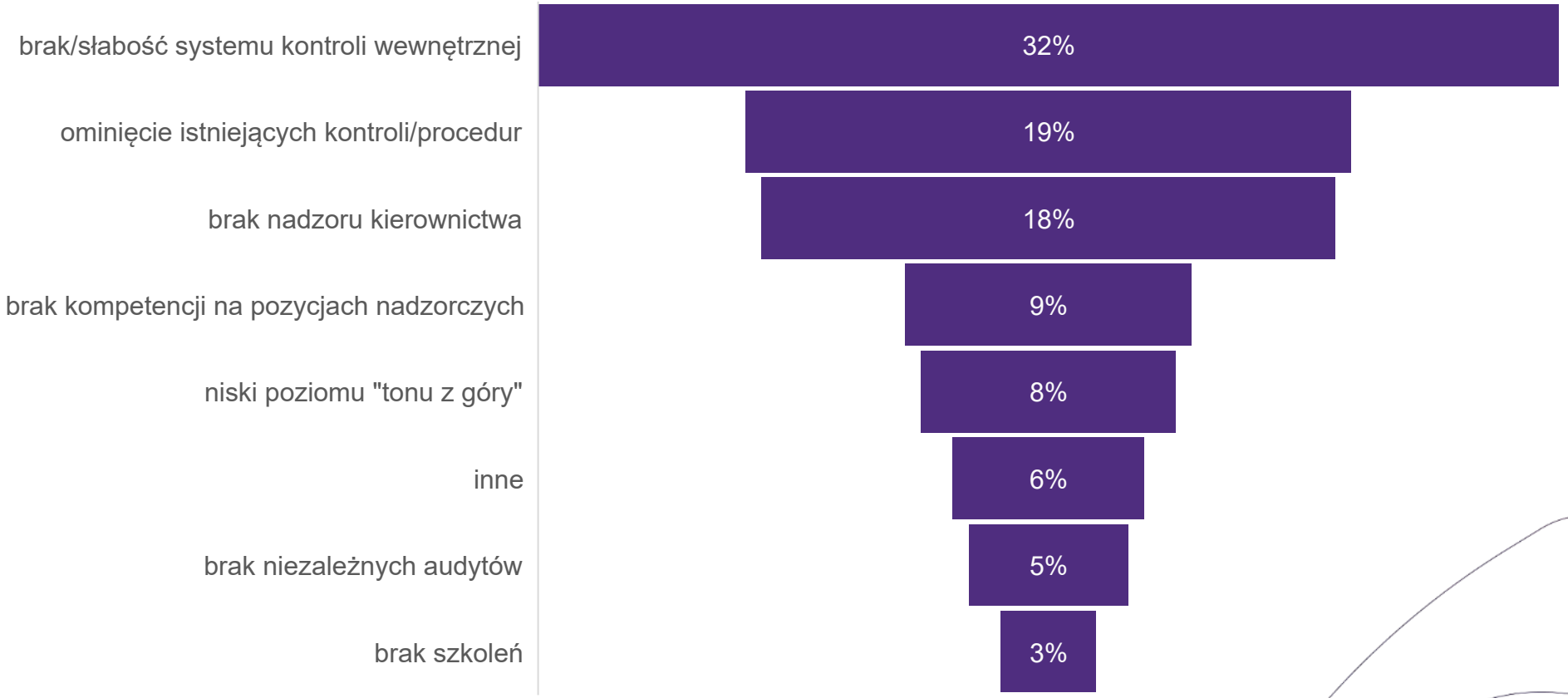


Źródło: Occupational Fraud 2024: A Report to the Nations. Copyright 2024 by the Association of Certified Fraud Examiners, Inc.

Grant Thornton

Oszustwa i nadużycia w liczbach

Jakie są najczęstsze powody występowania oszustw i nadużyć?



Źródło: Occupational Fraud 2024: A Report to the Nations. Copyright 2024 by the Association of Certified Fraud Examiners, Inc.

Grant Thornton

Jak odpowiedzieć na ryzyko oszustw i nadużyć?

Ryzyko oszustw i nadużyć może być zaadresowane podobnie jak inne ryzyka biznesowe.

- Akceptacja ryzyka (podejście niezalecane, a przynajmniej bez próby skwantyfikowania prawdopodobieństwa wystąpienia i skali wpływu potencjalnego zdarzenia na jednostkę).
- Unikanie ryzyka.
- Ubezpieczenie się od ryzyka.
- Aktywne zarządzanie ryzykiem
  - wymaga procesu oszacowania ryzyka m.in. w podziale na rodzaje oszustw i nadużyć, na działy, lokalizacje itp.
  - wymaga wdrożenia procedur oraz czynności kontrolnych adresujących ryzyko (w tym wdrożenie kodeksu etyki, zasad dotyczących realizacji zamówień i zakupów, zasad dotyczących pokrywania kosztów delegacji, zasad przeglądów istotnych bądź nietypowych transakcji)
  - wymaga prowadzenia okresowych szkoleń pracowników
  - wymaga okresowego przeglądu ryzyka oraz przeglądu stosowanych procedur i zasad
  - wymaga wdrożenia skutecznych kanałów anonimowego informowania o podejrzeniach oszustw i nadużyć

Studium przypadku 1

Zagranie all-in

Firma XYZ posiadała bardzo rozbudowany system kontroli wewnętrznej nad zakupami i płatnościami. Wszystkie płatności do kontrahentów procesowano z wykorzystaniem paczek przelewów generowanych z systemu ERP, wszystkie faktury zakupowe wymagały wielostopniowej weryfikacji, zanim w ogóle była możliwość „zaciągnięcia" ich do paczek przelewów.

Dodawanie kontrahentów do bazy danych systemu ERP wymagało podwójnej autoryzacji, podobnie jak modyfikowanie kluczowych danych (takich jak numer rachunku bankowego). Dodatkowo każdego miesiąca pracownik kontrolingu weryfikował próbę transakcji zmieniających dane w bazie danych dostawców z dokumentami źródłowymi, zapewniając dodatkowy element kontrolujący zasadność zmiany. Wydawało się, iż firma XYZ jest skutecznie zabezpieczona przed nieprawidłowościami w tym obszarze.

Pewnego dnia okazało się, że wszystkie kontrole można było „obejść" jednoosobowo, z wykorzystaniem aplikacji „Notatnik" systemu Windows.

Pracownik działu płatności zauważył, iż paczki przelewów generowane z systemu ERP mają format .txt. W ramach eksperymentu podwyższył o złotówkę kwotę płatności dla pojedynczej transakcji w jednej z paczek przelewów, system bankowy nie wygenerował błędu przy imporcie paczki. Zamiana danych oraz numerów rachunków bankowych kontrahentów w pliku .txt także nie spowodowała problemów.

Po krótkich przygotowaniach, na dzień przed urlopem, w dniu, w którym notowano w firmie najwięcej płatności pracownik podmienił w pliku .txt nazwę oraz numery rachunków bankowych kilku kontrahentów na łączną kwotę ponad 2 mln zł. Zastosował dane oraz numer rachunku bankowego założonych przez siebie firm, o podobnych nazwach do kluczowych kontrahentów firmy XYZ. Rachunki zostały zgłoszone do US i ujęte na białej liście. Osoba autoryzująca paczkę płatności w systemie bankowym nie wykryła modyfikacji – nie było oczywiście możliwe indywidualne sprawdzenie każdej z 120 transakcji zawartych w paczce. Ogólna kwota przelewów w systemie bankowym zgadzała się z podsumowaniem paczki płatności widocznym w systemie ERP, nic nie wskazywało na nieprawidłowości. Oszustwo zostało wykryte 5 dni później, na poziomie księgowania wyciągów bankowych – księgowa zauważyła, że nazwy firm, do których wykonano płatności nie zgadzają się w 100% z nazwami kontrahentów w bazie danych dostawców. Pracownik działu płatności nigdy nie wrócił z urlopu.

Studium przypadku 1

Zagranie all-in

Co poszło nie tak?

– W firmie XYZ stosowano zdecentralizowane podejście do systemu kontroli wewnętrznej – czynności kontrolne były wykonywane przez niezwiązanych ze sobą pracowników firmy, proces był podzielony pomiędzy różne komórki organizacyjne. Nie utworzono komórki audytu wewnętrznego. Istniało wiele rodzajów kontroli, które jednak całościowo nie ograniczyły wystarczająco możliwości wystąpienia oszustwa. Zabrakło spojrzenia całościowego audytora wewnętrznego, który monitorowałby okresowo zaprojektowanie i działanie systemu kontroli wewnętrznej w firmie i prawdopodobnie dostrzegłby lukę w procesie. **W opisanym przypadku możliwe jest zastosowanie następujących rozwiązań:**

– Wyeliminowanie kroku eksportu/importu paczki przelewów pomiędzy systemem bankowym i systemem ERP. Zwykle jest możliwe wdrożenie integracji systemów bankowych i systemów ERP, polegające na automatycznej transmisji paczek przelewów pomiędzy systemami, pracownik działu płatności traci możliwość edytowania raz wygenerowanej paczki

– Modyfikacja ustawień systemu ERP, w celu generowania paczek w formacie nieedytowalnym z wykorzystaniem podstawowych narzędzi systemowych. Dostawcy systemów (zwłaszcza starsze oprogramowanie kadrowo-płacowe) nie zawsze jednak oferują takie rozwiązanie. Opcją alternatywną jest wypracowanie własnego rozwiązania IT, które polegałoby na szyfrowaniu generowanych paczek płatności.

Studium przypadku 2

Historia jednego podpisu

Pani Ania pracowała w firmie „X” przez 30 lat, praktycznie od początku jej istnienia. Firma „X” jest spółką produkcyjną, posiada od dawna nieaktualizowany system finansowo-księgowy, nikt nie widział nigdy potrzeby jego zmiany. „X” to firma rodzinna, właściciele firmy są zżyci ze stałymi pracownikami.

Pani Ania prowadziła księgowość samodzielnie, druga księgowa odpowiadała głównie za system kadr i płac. Pani Ania cechowała się niezwykłą sprawnością działania – jednoosobowo wprowadzała i autoryzowała przelewy w systemie bankowym, oszczędzając czas wyższego kierownictwa. Z zaksięgowaniem wyciągu bankowego także nie miała nigdy żadnych problemów. Pani Ania często skarżyła się koleżankom, że jej wypłata nie odpowiada szerokiemu zakresowi jej obowiązków.

Po odejściu na zasłużoną emeryturę i otrzymaniu solidnej odprawy Pani Ania zapadła się pod ziemię, a wraz z nią cenna wiedza o procesach księgowych w firmie. Jak się okazało później - nie tylko to zniknęło bezpowrotnie.

Nowa księgowa zauważyła, że ilość transakcji rejestrowanych na jednym z kont należących do „pozostałych kosztów rodzajowych” zmalała o 97% w porównaniu do lat poprzednich. Zapytanie wysłane do pozostałych osób z pionu finansowego nie przyniosło żadnych efektów – nikt nie wiedział, jaki był powód transakcji rejestrowanych na koncie „inne koszty rodzajowe – łącznie”.

Po krótkim śledztwie okazało się, że Pani Ania w ciągu ostatnich 10 lat swojej pracy zdefraudowała prawie 300 tys. zł, których nikt się nigdy nie doliczył. Pięć miesięcznych, nieautoryzowanych płatności na niskie kwoty ginęło w zestawieniu ponad 200 uzasadnionych płatności za rzeczywiste faktury. Rozchody gotówki były księgowane drugostronnie na specjalnie utworzone, kosztowe konto księgi głównej. Transakcje opiewające na podobne, kwoty nieistotne dla jednostki nie wzbudzały podejrzeń.

Studium przypadku 2

Historia jednego podpisu

Co poszło nie tak?

Przebieg czynności w procesie nigdy nie powinien wyglądać tak, jak to miało miejsce w przypadku firmy „”X” – zabrakło podstawowej segregacji obowiązków. W żadnym wypadku nie jest uzasadniona sytuacja, gdy księgowa jest odpowiedzialna za wprowadzenie przelewu, jego autoryzowanie, a także księgowanie wyciągów bankowych. Dodatkowo archaiczny system finansowo-księgowy pozwalał na swobodne dodawanie nowych kont księgi głównej oraz nie narzucał ograniczeń w wyborze konta drugostronnego w transakcjach rozchodu środków pieniężnych. Podstawowym błędem Pani Ani było rejestrowanie transakcji na odrębnym koncie księgowym – transakcje najczęściej skuteczniej ukrywane są w takich przypadkach na kontach odchyleń od kosztu standardowego lub kontach usług obcych.

Ryzyko podobnych zdarzeń pozwoliłoby ograniczyć:

– rozdzielenie obowiązków wprowadzania przelewów, autoryzacji przelewów oraz księgowania wyciągów bankowych,

– wprowadzenie niezależnej autoryzacji transakcji bankowych przez inne osoby niż te wprowadzające dane do przelewów lub te zamawiające dany zakup na podstawie dokumentacji uwierzytelniającej powód płatności,

– procesowanie przelewów z wykorzystywaniem generowanych z systemu „paczek płatności”, które następnie są importowane bezpośrednio do systemów bankowych na bazie danych wcześniej wprowadzonych do baz danych kontrahentów oraz systemów workflow.

Grant Thornton

Studium przypadku 3

Koszmar pilnej płatności

Firma XYZ jest firmą produkcyjną, która wykorzystuje w recepturach materiałowych 6 kluczowych surowców. Większość pracowników biurowych wzięła urlop na czas długiego weekendu majowego, jednak produkcja cały czas szła pełną parą. W trakcie urlopu dyrektor działu zakupów został zasypany smsami przez dyrektora produkcji – jeden z kluczowych surowców był na wyczerpaniu i w przypadku braku jego dostawy w ciągu najbliższych 2 dni produkcja uległaby zatrzymaniu.

Dostawcy firmy XYZ mają w umowach 10 dni na przetworzenie zamówienia, proces ten mogłaby przyspieszyć jedynie przedpłata.

W firmie XYZ wszystkie przedpłaty procesowane są z wykorzystaniem systemu workflow. Kwota przedpłaty była istotna, więc system workflow automatycznie przypisał 4 weryfikatorów takiego wniosku. Okazało się, że część z nich była niedostępna, proces w workflow uległ zatrzymaniu.

Po uzyskaniu telefonicznej zgody zarządu, dyrektor działu zakupów wydał specjaliście ds. płynności polecenie wykonania płatności „ manualnej” do kontrahenta – wprowadzonej ręcznie w systemie bankowym, z pominięciem procesu tworzenia paczek przelewów. Płatność ta została wykonana. Nikt jednak nie zwrócił uwagi, że dzień później przeprocesowano w pełni wniosek o przedpłatę w workflow. Autoryzowany wniosek o przedpłatę stał się widoczny w systemie ERP (występowała integracja ERP oraz workflow) dla asystenta ds. płatności, który następnie zaciągnął go do paczki płatności.

Kwota oraz ilość przelewów po przerwie urlopowej była bardzo duża, nikt nie zwrócił uwagi przy autoryzacji płatności w systemie bankowym na pojedynczą przedpłatę. Płatność została wykonana podwójnie.

Studium przypadku 3

Koszmar pilnej płatności

Co poszło nie tak?

W większości firm co jakiś czas pojawiają się płatności „pilne” – np. konieczność wpłaty wadium przetargowego, przedpłaty na dostawę kluczowych surowców, wpłacenie opłaty administracyjnej blokującej dalsze procesowanie sprawy. **W firmie XYZ zabrakło 2 podstawowych elementów w systemie kontroli wewnętrznej:**

– Nie występowały skuteczne mechanizmy kontroli wewnętrznej nad poziomem stanów magazynowych kluczowych surowców – informacja trafiła do departamentu zakupów zbyt późno. Najczęstszym rozwiązaniem jest ustalenie minimalnych stanów magazynowych kluczowych surowców. Zwykle system ERP można skonfigurować w taki sposób, iż będzie wysyłał automatyczne ostrzeżenia w momencie osiągnięcia poziomów minimalnych

– Nie występowała „skrócona” ścieżka w workflow, która mogłaby mieć zastosowanie do transakcji o pilnym charakterze czasowym. W niektórych przypadkach transakcje wymagają błyskawicznego przeprocesowania i kroki autoryzacyjne mogłyby być ograniczone do osoby z zarządu. Nie wystąpiłaby konieczność „obejścia” systemu w sytuacji awaryjnej z wykorzystaniem e-maili, telefonów, ustnych zatwierdzeń. Wyeliminowałoby to u źródła powód wystąpienia podwójnej płatności w firmie XYZ

Podsumowanie

Ryzyko oszustw i nadużyć pracowniczych jest nieodłącznym ryzykiem w prowadzonej działalności. Jego poziom może się różnić na przestrzeni lat i zwykle wzrasta w okresach dekoniunktury lub w sytuacji gdy wzrosty wynagrodzeń nie nadążają za inflacją.

Według badań ACFE 29% oszustw i nadużyć pracowniczych wynika ze słabości systemu kontroli wewnętrznej, a kolejne 20% przypadków wynika z omijania wdrożonych już kontroli.

Ryzykiem oszustw i nadużyć pracowniczych można zarządzać. Takie zarządzanie wymaga jednak świadomej analizy występujących zagrożeń oraz zaprojektowanie i wdrożenie odpowiednich odpowiedzi na oszacowane ryzyko
(w tym wdrożenie odpowiednich procedur i kontroli).

Najskuteczniejszą metodą w wykrywaniu oszustw i nadużyć pracowniczych jest system anonimowego informowania o podejrzanych praktykach (whistleblowing).

Zapraszam do kontaktu

CLIENT WEEK
z Grant Thornton

Marek Błażejewski

Manager, Business Risk Serivces
Grant Thornton

E marek.blazejewski@pl.gt.com

M +48 691 710 411

Na co dzień dzielimy się wiedzą na:

GrantThornton.pl

Znajdą tam Państwo między innymi cykl artykułów na temat oszustw i sprzeniewierzeń, publikujemy też raport na temat corporate governance w spółkach notowanych na GPW.

Zapraszamy też do zapisu na newsletter.