

# **Jak napisać dobre *issue* audytowe?**

---

Warszawa, 25.11.2019r.

- **Dlaczego dobrze napisane *issue* jest ważne?**
- **Jak zidentyfikować dobre *issue*?**
- **Czy *issue* to na pewno *issue*?**
- **Jeśli *issue* to na pewno *issue*, to jak je dobrze opisać?**
- **Warsztat: napisz dobre *issue***

## Dlaczego dobrze napisane *issue* jest ważne?

Odbiorcy-czytelnicy raportów audytowych mają różne oczekiwania  
... oraz są bardzo zajętymi ludźmi i powinni otrzymać najistotniejsze informacje

<b>średnia kadra zarządcza funkcje liniowe</b>	<ul style="list-style-type: none"><li>• szczegółowe informacje i rekomendacje pozwalające na zmitigowanie issue</li><li>• poziom i znaczenie ryzyka, co wpływa na priorytety i budżet na działania naprawcze</li></ul>
<b>zarząd, wyższa kadra zarządcza</b>	<ul style="list-style-type: none"><li>• informacje na wyższym poziomie ogólności,</li><li>• przegląd kluczowych ryzyk i issues</li></ul>
<b>Komitety Audytu</b>	<ul style="list-style-type: none"><li>• informacje o:<ul style="list-style-type: none"><li>○ sprawozdawczości finansowej,</li><li>○ zgodności z przepisami,</li><li>○ systemie kontroli wewnętrznej,</li><li>○ systemie zarządzania ryzykiem</li></ul></li></ul>
<b>regulator</b>	<ul style="list-style-type: none"><li>• może zażądać raportów w celach kontrolnych</li></ul>

*„zawsze wejdź w buty czytelnika”*

## Dlaczego dobrze napisane *issue* jest ważne?

---

### Dobrze napisane *issue*:

- ✓ pozwala czytelnikom szybko i łatwo zrozumieć
  - gdzie się pojawił i na czym polega problem
  - dlaczego istotne jest jego zaadresowanie
- ✓ buduje wizerunek audytu wewnętrznego jako
  - partnerskiej, silnej merytorycznie funkcji wspierającej biznes oraz realizację strategicznych celów organizacji
  - komórki, która rozumie biznes i organizację

4 razy jako **ZAGADNIENIE**

w tym raz jako kategoria zagadnień,  
które w angielskiej wersji są  
wymienione 3 razy

3 razy jako **KWESTIA**

W wersji angielskiej Standardów słowo *issue*  
pojawia się 12 razy i zostało przetłumaczone

1 raz jako **PROBLEM**

2 razy w odniesieniu do  
czasownika wydać,  
wystawić, opracować  
(to nas dzisiaj nie interesuje)

## Dlaczego dobrze napisane *issue* jest ważne? - Standard 2060 IIA

### Reporting to Senior Management and the Board

- The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan and on its conformance with the Code of Ethics and the Standards. **Reporting must also include significant risk exposures and control issues**, including fraud risks, governance issues, and **other matters that require the attention** of senior management and/or the board.

### Składanie sprawozdań kierownictwu wyższego szczebla i radzie

- Zarządzający audytem wewnętrznym musi składać kierownictwu wyższego szczebla i radzie okresowe sprawozdania na temat celu działania audytu wewnętrznego, uprawnień, odpowiedzialności, stopnia wykonania planu oraz zgodności z Kodeksem etyki i Standardami. **Sprawozdania muszą również obejmować zagadnienia dotyczące systemu kontroli, ładu organizacyjnego, znaczącego ryzyka**, na jakie narażona jest organizacja (w tym ryzyka oszustwa) oraz **inne, które wymagają uwagi** kierownictwa wyższego szczebla i/lub rady.

## Dlaczego dobrze napisane *issue* jest ważne? - Standard 2410 IIA

### Criteria for Communicating

Communications must include the engagement's objectives, scope and results.

### Kryteria informowania

Informacja musi obejmować cele, zakres i wyniki zadania.

### Jakość informacji

- Przekazywane informacje muszą być dokładne, obiektywne, jasne, zwięzłe, konstruktywne, kompletne oraz dostarczone na czas.

### Quality of Communications

- Communications must be accurate, objective, clear, concise, constructive, complete, and timely.



## Dlaczego dobrze napisane *issue* jest ważne? - Standard 2440 IIA

### Przekazywanie wyników

Zarządzający audytem wewnętrznym musi przekazać wyniki właściwym osobom.

### Disseminating Results

The chief audit executive must communicate results to the appropriate parties.

## Dlaczego dobrze napisane *issue* jest ważne? - Standard 2450 IIA

### Ogólne opinie

- Jeśli wydawana jest ogólna opinia, musi uwzględniać strategię, cele i ryzyko organizacji oraz oczekiwania kierownictwa wyższego szczebla, rady i innych interesariuszy. Ogólna opinia musi być poparta wystarczającymi, rzetelnymi, przydatnymi i dotyczącymi zadania informacjami.

### Overall Opinions

- When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information.

## Jak zidentyfikować dobre *issue*?

---

Aby napisać, najpierw należy:

**Zidentyfikować**  
„dobre”,  
właściwe,  
istotne, ...

*issue* w toku  
prac  
audytowych :)

### Jeśli „dobry” audyt, to należy ...

- dostosować strategię audytu do strategii organizacji (*wspierać ją*)
- zrozumieć audytowany obszar i związane z nim ryzyka, np:
  - zmiany w otoczeniu prawnym
  - zmiany w przebiegu procesu/-ów
  - cele procesu/-ów,
  - punkty styku z innymi procesami
  - nieprawidłowości zidentyfikowane przez I oraz II linię obrony
  - obszary troski/zainteresowań kadry menedżerskiej
- przygotować plan/program audytu adresujący najważniejsze zidentyfikowane ryzyka
- pamiętać o celu audytu
- zidentyfikować „dobre”: właściwe, istotne *issue*

## Co to jest *issue*?

---

*Issue* to opis defektu, luk, wad w mechanizmach kontrolnych.  
Jest to fakt, stwierdzenie istniejących nieprawidłowości.

- ✓ koncentruje się na zadaniu lub procesie, które:
    - nie jest realizowane
    - jest realizowane nieprawidłowo albo w niewystarczający sposób
    - nie pozwala na zmitigowanie ryzyka
  - ✓ może dotyczyć nieprawidłowego ...
    - zaprojektowania (*design*)
    - wykonywania (*operation*)
    - skuteczności (*effectiveness*)
- ... mechanizmu kontrolnego.

## Czy *issue* to na pewno *issue*?

---

- ✓ *Issue* wiąże się z istotnym negatywnym wpływem/skutkiem dla organizacji. Skutek może być rozpatrywany w różnych wymiarach, np:
- finansowym
  - regulacyjnym
  - reputacyjnym
  - obsługi/satysfakcji klienta
  - operacyjnym/efektywnościowym

**Zanim  
zacznieš pisać  
upewnij się, że**

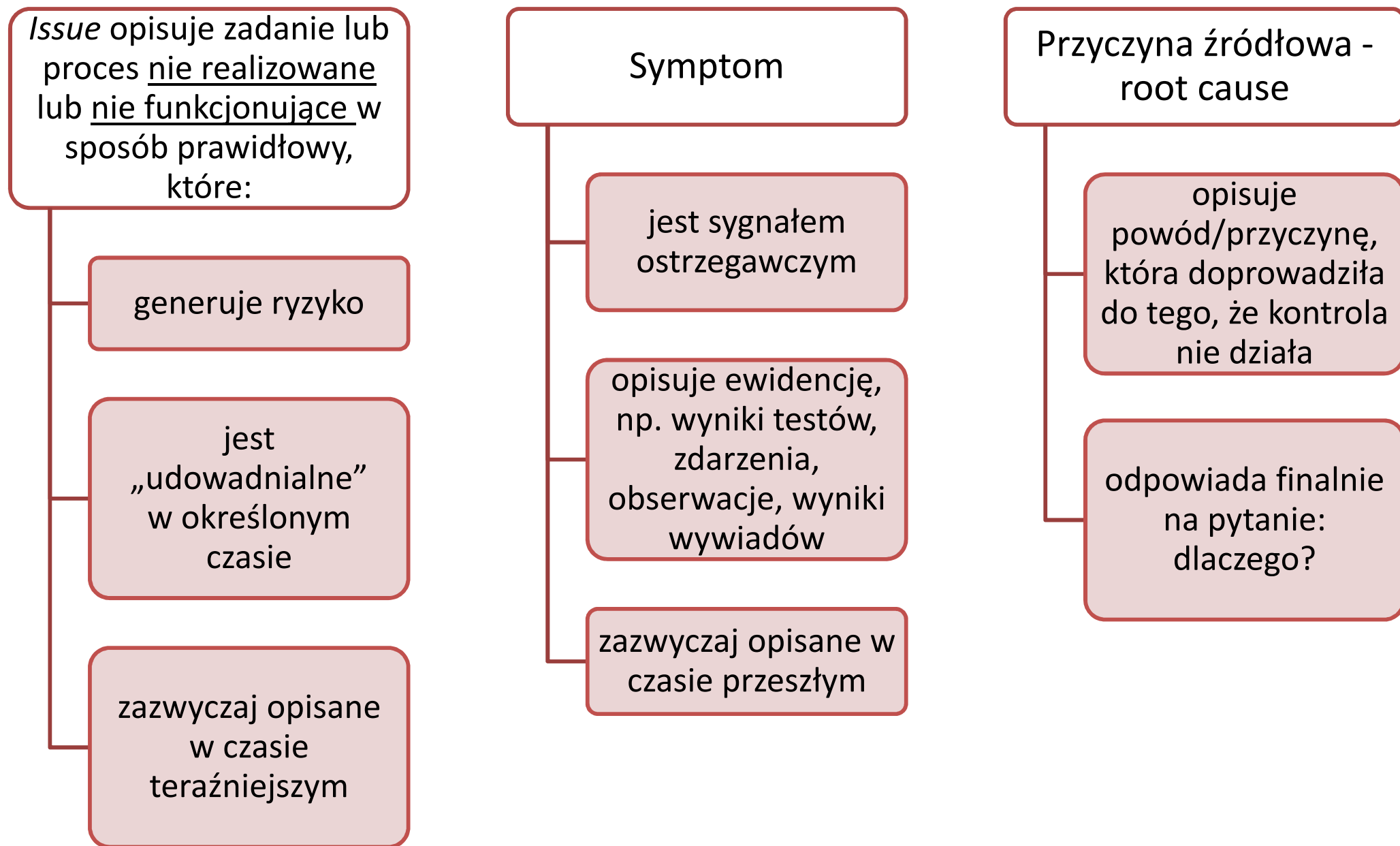
- znalezisko to na pewno *issue*
- a może jednak obserwacja?

**Jeśli to tylko  
obserwacja to**

...

- czy może być przekazana  
w innej formie?

## Jak opisać *issue*? Różnice: *issue* - *symptom* - *root cause*





## Jak zidentyfikować przyczynę źródłową - *root cause*?

---

- Identyfikacja przyczyny źródłowej (*root cause*) jest **kluczowa** dla znalezienia odpowiedniego rozwiązania/planu naprawczego.
- Pomocne jest zadawanie pytania **dlaczego**
  - dlaczego to się stało?
  - dlaczego coś nie zostało zrobione choć powinno?
  - co do tego doprowadziło?
  - jaka jest przyczyna?
- Należy zadawać sobie pytanie tak długo, aż zostanie zidentyfikowana **pierwotna** przyczyna nieprawidłowości. To jest **przyczyna źródłowa**, do której powinien być przygotowany plan naprawczy.

## Jak zidentyfikować przyczynę źródłową - *root cause*?

---

- Przydatne jest przygotowanie i wykorzystywanie wystandaryzowanego „katalogu” przyczyn źródłowych.
- Skonsultować/omówić z audytowanym
- O ile jest taka możliwość zweryfikować na „organizmie”

Umożliwia to późniejsze analizy i wnioskowanie na poziomie zagregowanym.

### Zasady: 4C / 3C + I

- ✓ **Criteria (kryteria, wymagania):** stan oczekiwany, co było wymagane, co powinno zostać zrobione
- ✓ **Condition (stan faktyczny):** co się zepsuło, co nie zostało zrobione
- ✓ **Cause (przyczyny):** z jakiego powodu (dlaczego) coś się zepsuło, nie zostało zrobione, ekspozycja na luki pomiędzy stanem oczekiwany a faktycznym
- ✓ **Consequence / Impact (konsekwencja / wpływ):** dlaczego *issue* jest ważne, ryzyko dla organizacji: np. finansowe, operacyjne, regulacyjne

## Jak opisać issue? **Zasada 4C** - przykład

### Condition / Stan faktyczny

- Dwie płatności na rzecz dostawców w wysokości przekraczającej 5.000 EUR zostały niewłaściwie zatwierdzone.

### Cause / Przyczyna

- Błąd techniczny powstały po instalacji ostatniej aktualizacji oprogramowania w systemie XYZ spowodował, że płatności zostały wykonane po uzyskaniu wyłącznie jednego poziomu akceptacji.

### Criteria / Kryteria

- Polityka firmy wymaga zatwierdzenia każdej płatności przekraczającej 5.000 EUR przez dwie osoby.

### Consequence / Skutek

- Niewłaściwa akceptacja może prowadzić do wykonania błędnych lub oszukańczych płatności.

## Jak opisać issue? Zasada 3C+I - przykład

### Criteria / Kryteria

- Istniejące w organizacji Polityki/Procedury wymagają zatwierdzenia każdej płatności przekraczającej 5.000 EUR przez dwie osoby.

### Condition / Stan faktyczny

- Dwie płatności na rzecz dostawców w wysokości przekraczającej 5.000 EUR zostały zatwierdzone przez jedną osobę.

### Cause / Przyczyna

- Błąd techniczny powstały po instalacji ostatniej aktualizacji oprogramowania w systemie XYZ spowodował, że płatności zostały wykonane po uzyskaniu wyłącznie jednego poziomu akceptacji.

### Impact / Wpływ

- Brak poprawnego funkcjonowania w systemie schematu akceptacji płatności może prowadzić do wykonania niepoprawnych lub oszukańczych płatności.

- Opisując *issue* należy uwzględnić:
  - Mechanizmy kontrolne o charakterze kompensującym, które mogą pomóc obniżyć wycenę *issue* (jednak może to wymagać dodatkowego testowania ich zaprojektowania i operacyjnej efektywności)
  - Kwestie zidentyfikowane przez kadrę zarządzającą, które mogą stanowić dowód działania mechanizmów kontrolnych w I lub II linii obrony (ich oddzielne opisywanie w raporcie może nie być wymagane, poza przywołaniem w opinii)

## Jak opisać *issue*? Segregation of duties i brak dowodów

- Jak sformułować obserwację dotyczącą „Segregation of Duties”?

Najlepiej unikać sformułowania SoD gdyż jest to kategoria kontroli natomiast nie opisuje konkretnej luki. Najbardziej czytelne byłoby wskazanie na czym polega konflikt.

Przykład:

Ta sama osoba aktualizuje dane w kartotece kontrahenta oraz jednocześnie autoryzuje polecenie przelewu i uzgadnia rachunki bankowe.

- Jak sformułować opis *issue* / obserwacji audytowej w przypadku braku dowodu na realizację kontroli?

Brak dowodu jest symptomem. Ponieważ istotne jest koncentrowanie się na konkretnej czynności warto rozważyć różne scenariusze, jednak zawsze koncentrując się na faktach.

Przykład:

- Kierownictwo nie przedstawiło dokumentacji ewidencjonującej przeprowadzenie kontroli
- Kierownictwo nie dokumentuje procesu monitorowania
- Kierownictwo nieregularnie dokumentuje, itp.

Opisując *issue* warto:

- ✓ używać **prostego języka**
- ✓ pisać **do odbiorcy** a nie od nadawcy
- ✓ używać **strony czynnej**
- ✓ formułować **krótkie zdania**, unikać **wtrąceń**, zdań wielokrotnie złożonych
- ✓ unikać **żargonu i skrótów** zrozumiałych jedynie dla nielicznych czytelników (chyba że są niezbędne i zostały wcześniej odpowiednio zdefiniowane)
- ✓ unikać **nadmiernego poziomu szczegółowości i obwiniającego tonu**
- ✓ po napisaniu *issue* **przeczytać** je raz jeszcze (najlepiej na głos) i **wykreślić wszystkie wyrazy**, których usunięcie nie wpływa na znaczenie zdań



Opisując *issue* warto:

- ✓ Stosować konsekwentne **zasady prezentacji** (przyjęty wzór, format!)
  - to duże ułatwienie dla czytelników, jeśli każdy raport ma taki sam układ, a *issues* są zawsze opisywane w takiej samej formie
- ✓ Stosować **spójne i konsekwentne zasady wyceny *issue***
  - to wyklucza uznaniowość i arbitralność
- ✓ Zastanowić się, **czy można zgrupować poszczególne *issues* w podobne kategorie** i ograniczyć ich liczbę
  - to ułatwi również późniejsze nimi zarządzanie
- ✓ Jeśli to możliwe - **zastosować wizualizacje (np. przebieg procesu)**
  - to ułatwi odbiorcom zrozumienie istoty *issue*

## Issue opisywane w języku angielskim – *readability score*

- dla raportowania w języku angielskim można skorzystać ze sprawdzenia tzw. *Flesch–Kincaid readability tests*, czyli zweryfikować jak zrozumiałe dla odbiorcy jest to, co napisałeś.
- opcja jest dostępna w edytorze Word (Review/Spelling & Grammar)

READING EASE	READING LEVEL BY GRADE	% OF PEOPLE WHO UNDERSTAND THE WRITING	BY MAGAZINE
Difficult	16 15 14	5%	No popular magazines
Fairly Difficult	13 12 11	25%	Scientific American The Economist
Average	10 9 8	50%	Wall Street Journal Vanity Fair
Fairly Easy	7		Popular Novels
Easy	6	95%	Comics

## Issue opisywane w języku angielskim – *readability score*

### Readability Statistics

?

×

#### Counts

Words	2,642
Characters	15,856
Paragraphs	283
Sentences	58

#### Averages

Sentences per Paragraph	1.6
Words per Sentence	23.8
Characters per Word	5.5

#### Readability

Flesch Reading Ease	23.4
Flesch-Kincaid Grade Level	15.7
Passive Sentences	37.9%

OK

- ✓ dla raportowania w języku polskim można skorzystać ze sprawdzenia tzw. *Indeksu mglistości tekstu*, czyli zweryfikować ile lat nauki potrzebuje odbiorca aby zrozumieć to zagadnienie.
  - [www.jasnopis.pl](http://www.jasnopis.pl)
  - [www.logios.pl](http://www.logios.pl)

---

**Dziękujemy za uwagę  
i zapraszamy na  
warsztaty!!!**



### Przykład symptomu:

*Raport ze strukturą wiekową oraz statusem szkód zawiera dużą liczbę pozycji ze statusem „otwarta”.*

- Jaka będzie obserwacja audytowa?
- Co będzie naszym *issue*?
- Jeśli audit *issue* opisuje symptom zamiast faktyczne *issue* (lukę kontrolną) – jakie ryzyko to kreuje?

### Przykład 1:

*Znajdujesz niepoprawne dane w kalkulacji taryfy/składki*

*Czy to issue, symptom czy przyczyna źródłowa (root cause)?*

*Rozwiązanie:*

*Symptom: Niepoprawne dane w kalkulacji taryfy/składki*

*Issue: Manager nie przegląda regularnie jakości danych taryfikacyjnych*

*Root cause: Procedura operacyjna nie uwzględnia częstotliwości przeglądów managerskich (po prostu nigdy wcześniej o tym nie pomyśleli)*

## Warsztat - wprowadzenie

---

### Przykład 2:

**Symptom:** W próbie wybranych 25 aktywnych profili użytkowników identyfikujesz 3 zdublowane profile, 4 profile osób nie będących już pracownikami, kilka niekompletnych wniosków niepodpisanych przez przełożonych.

*Co do tego doprowadziło?*

**Kolejne symptomy:** Ostatni przegląd profili miał miejsce 20 miesięcy wcześniej. IT nie wiedziało, że pracownicy nie pracują. IT nie potrafiło wytłumaczyć dlaczego formularze są niekompletne i nie zawierające podpisu managera.

*Co do tego doprowadziło?*

**Root cause:** Procedura nie zawiera wymogu w zakresie regularnego przeglądu uprawnień/profili (przyczyną tego może być niekompetencja lub zaniedbanie) kolejne pytania już nie będą potrzebne.

Manager myślał, że informacja o odchodzących pracownikach jest przekazywana przez kadry do IT (kolejne pytanie nie będzie konieczne)

Manager nie wiedział, że miał podpisać formularz.

**Issue:** Kierownictwo nie przegląda regularnie profili.

IT nie otrzymuje informacji o pracownikach, którzy odchodzą w celu dezaktywacji uprawnień / HR nie przekazuje informacji o odchodzących pracownikach.



### Przykład 3:

*Które z poniższych zdań opisuje w poprawny sposób lukę kontrolną (issue)?*

- 1. Narzędziem do monitorowania wydajności systemu nie dostarcza odpowiednich wskaźników i mierników dla systemu XYZ*
- 2. IT nie monitoruje wydajności systemu XYZ*

**A teraz zachęcamy do pracy nad konkretnymi przykładami**