



## Instrukcja użytkowania aplikacji AnRisk

27 września, 2024

## Spis treści

Spis treści .....	2
Dashboard.....	3
Dodanie procesu.....	4
Edycja komponentu.....	8
Edycja ryzyka. ....	10
Filtrowanie ryzyk w zakładce ocena ryzyka.....	11
Ocena ryzyka.....	13
Raportowanie.....	15
Przegląd ryzyka.....	16
KRI – Jednostki miar Key Risk Indicators (kluczowe wskaźniki ryzyka).....	17
Dodanie KRI do ryzyka. ....	18
KRI – Pomiar.....	20
Raportowanie KRI.....	20
Klasyfikacja komponentów.....	21
Klasyfikacja komponentu w kontekście procesu.....	21
Klasyfikacja informacji.....	22
Zarządzanie incydentami .....	23
Konfiguracja.....	23
Rejestracja incyduentu.....	26

## Wprowadzenie.

Ten dokument stanowi przewodnik użytkownika aplikacji dedykowanej do samodzielnej analizy ryzyka. Aplikacja została zaprojektowana w celu umożliwienia użytkownikom skutecznego i efektywnego przeprowadzania analizy ryzyka, w różnych kontekstach działalności. Zawiera ona krok po kroku instrukcje oraz narzędzia niezbędne do identyfikacji, oceny i zarządzania ryzykiem.

## Dashboard.

1. Informacje dostępne w Dashboard-ie aplikacji podzielone zostały na dwie grupy.
  - a. Komunikaty z aplikacji:
    - Informacje o nowych ryzykach on-line.
    - Ostrzeżenia o przekroczonym terminie realizacji planu postępowania.
    - Informacje o konieczności przeprowadzenia przeglądu ryzyk.
    - Informacje dotyczące wymaganych pomiarów KRI.
    - Informacje o realizacji zgłoszeń i incydentów.
    - Informacje dotyczące uprawnień.
  - b. Informacje statystyczne:
    - Statystyki ilości ryzyk ocenionych i nieocenionych.
    - Statystyki ilości ryzyk nieakceptowalnych i akceptowalnych.
    - Statystyki w odniesieniu do poziomu ryzyka.
    - Informację o ostatnio aktualizowanych ryzykach.
    - Statystyki dotyczące ilości ostatnio ocenionych ryzyk.
    - Statystyki dotyczące liczby zdefiniowanych ryzyk w ciągu ostatnich 12 miesięcy.

## Dashboard

### Komunikaty i ostrzeżenia

#### Ryzyka On-Line

[Sprawdź teraz](#)

Brak dostępnych aktualizacji.

Przekroczony termin realizacji planu postępowania z ryzykiem

[Istnieją przeterminowane ryzyka: 1](#)

Wykonanie przeglądu ryzyk

Nie ma przeglądów do wykonania.

Wykonanie pomiarów KRI

[Wymagane wykonanie pomiarów KRI: 105](#)

Realizacja zgłoszeń i incydentów

[Nowe zgłoszenia do realizacji: 12](#)

Wnioski o zmianę uprawnień

[Zakresy uprawnień oczekujące na akceptację: 13](#)

[Wnioski oczekujące na akceptację: 11](#)

[Wnioski zwrócone do poprawienia: 2](#)

[Wnioski oczekujące na realizacji: 5](#)

### Statystyki

Ryzyka zidentyfikowane: 332

Ocenione: 3

Nieocenione: 329

Poziomy ryzyka ogółem

Nieakceptowalne: 1

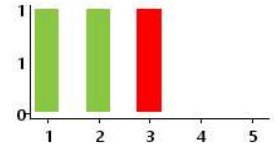
Akceptowalne: 2

Poziomy ryzyka szczegółowo

Poziom 1: 1 Poziom 4: 0

Poziom 2: 1 Poziom 5: 0

Poziom 3: 1



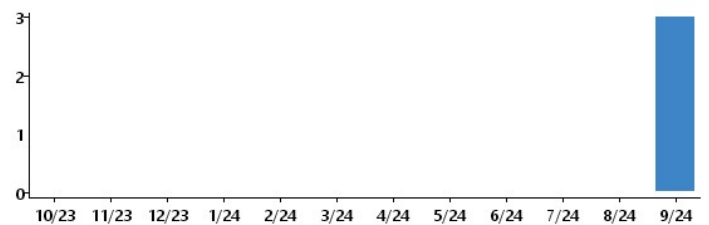
#### Ryzyka z przekroczonym terminem realizacji planu postępowania

Komponent	Data	Odpowiedzialny
Token	12.09.2024	Maciej

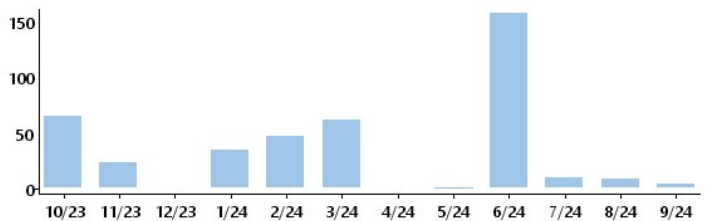
#### Ostatnio zaktualizowane ryzyka

Komponent	Data	Ocena wyk.
Token	13.09.2024	Tak
System e-BANK	11.09.2024	Tak
Pendrive	11.09.2024	Tak
Firewall (Zapora sieciowa)	06.09.2024	Nie
Dane osobowe	06.09.2024	Nie
Pracownik księgowości	05.09.2024	Nie
Pracownik księgowości	05.09.2024	Nie
System księgowy	05.09.2024	Nie

#### Liczba wykonanych ocen ryzyk w ciągu ostatnich 12 miesięcy

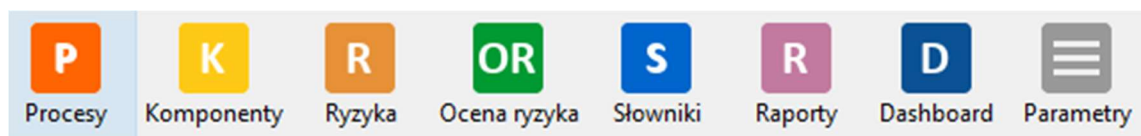


#### Liczba zidentyfikowanych ryzyk w ciągu ostatnich 12 miesięcy



## Dodanie procesu.

- Definicja procesów realizowana jest w zakładce „Procesy”.



- Identyfikacja procesów obejmuje:

- nazwę procesu,
- opis procesu,
- właściciela procesu,
- grupy przetwarzanych informacji (generowanych automatycznie),
- komórki organizacyjne realizujące proces (generowane automatycznie),
- miejsce realizacji procesu,
- informację o danych wrażliwych przetwarzanych w procesie,
- informację o komponentach wykorzystywanych w procesie,
- pole opisowe na dodatkowe uwagi,
- Znacznik aktywności procesu.



Aktywny – odznaczenie tego pola powoduje pomijanie procesu podczas zliczania statystyk oraz nie jest brane pod uwagę generując raporty.

### 3. Panel zakładki procesu.



**Ins – Dodaj** – umożliwia dodanie nowego procesu.

**Del – Usuń** – umożliwia skasowanie wybranego procesu.

**F4 – Edytuj** – pozwala na wprowadzenie zmian w procesie.

**F6 – Drukuj** – funkcja nieaktywna w tym widoku.

**F7 – Do Excela** – pozwala na eksport widocznych na ekranie procesów do aplikacji Excel.



**Del – Usuń** – pozwala skasować procesy, które nie zawierają żadnych ryzyk. Jeżeli w procesie znajdują się ryzyka należy je wcześniej usunąć.

### 4. Dodanie nowego procesu.

Nazwa: Księgowość		Komórki organizacyjne realizujące proces:		Komponenty wykorzystywane w procesie:	
Rodzaj: Istotny	Właściciel: Paweł Jakubiak (pawel.jakubiak@imns.pl)	DI - IT Informatyka WF - Płace Wydział Finansów		Dane osobowe Logi Pendrive Pracownik księgowości System e-BANK System księgowy Token	
Opis: Obsługa finansowo - księgowo		Dodatkowy opis / uwagi:			
Grupy przetwarzanych informacji (4): Dane finansowe Dane klientów Dane kontrahentów Dane pracowników		Miejsce realizacji procesu: lokalnie			

Dodanie nowego procesu wymaga wprowadzenia pola z **nazwą procesu**.



**Nazwa procesu** – najczęściej stosowane są dwie metody prowadzenia procesów w programie:

- Szeroka grupa ryzyk (jeden worek) w obrębie jednego procesu np. Nadzorowanie środowiska teleinformatycznego.
- Podzielenie obszarów na podprocesy np. Zarządzanie kopiami, Zarządzanie siecią, Zarządzanie helpdeskiem itp.

Program umożliwia wprowadzenie dodatkowych informacji do procesu (pola opcjonalne).

**Opis** – określenie działań/czynności realizowanych w procesie, wyników przeprowadzonych analiz BIA, DPIA itp.

**Kategorie przetwarzania danych osobowych** – informacje o typach danych, przetwarzanych w ramach procesu (dane pracowników, dane klientów, dane kontrahentów itp.).

**Właściciel** – przypisanie osoby odpowiedzialnej za proces.

**Miejsce realizacji procesu** – określa się miejsce, w którym dochodzi do przetwarzania (lokalnie, zdalnie, dane powierzone itp.).

**Dodatkowy opis / uwagi** – pole umożliwia wprowadzenie dodatkowych opisów.

**Dane szczególnie wrażliwe** – należy zaznaczyć, jeżeli w ramach procesu przetwarzane są dane określone w art. 9 RODO.

**Komórki organizacyjne realizujące proces** – komórki uzupełniane są automatycznie na podstawie komórek przypisanych do ryzyka w obrębie procesu.

**Komponenty wykorzystywane w procesie** – lista budowana jest automatycznie na podstawie komponentów przypisanych do ryzyka w obrębie procesu.

**Aktywny** – oznaczenie to pozwala na uwzględnienie procesu w raporcie i zmienia jego widoczność na liście procesów.



Zaznaczenie '**Dane szczególnie wrażliwe**' powoduje podniesienie wartości oceny utraty danych osobowych o n+1 (na zakładce Ocena ryzyka).

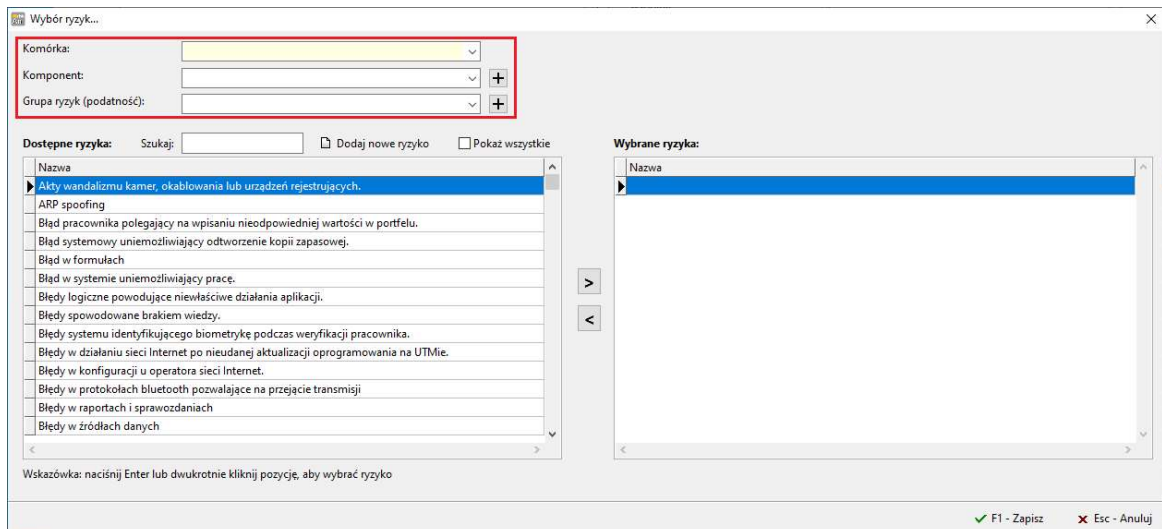
## 5. Lista ryzyk przypisanych do procesu.

Ryzyka związane z procesem (19):			
Komórka	Komponent	Grupa ryzyka	Ryzyko
DI - IT	Logi	Błędy administratora	Brak kopii zapasowej logów
DI - IT	Pendrive	Błędy pracownika	Usunięcie danych z nośnika
Informatyka	System księgowy	Uszkodzenie	Uszkodzenie systemu księgowego uniemożliwiające prace.
WF - Płace	Pracownik księgowości	Błędy pracownika	Przekazanie pracownikom informacji traktowanych jako poufne.
WF - Płace	Pracownik księgowości	Błędy pracownika	Wykorzystanie przekazanych danych do logowania do systemu księgowego nieuprawnionej osobie.
WF - Płace	Pracownik księgowości	Błędy pracownika	Zmiana konta bankowego na podstawie Phishingu.
WF - Płace	System e-BANK	Błędy pracownika	Utrata urządzenia służącego do potwierdzania przelewu.
WF - Płace	System e-BANK	Błędy pracownika	Wykonanie przelewu na nieodpowiedni nr konta bankowego.
WF - Płace	System e-BANK	Błędy pracownika	Wykonanie przelewu na nieodpowiednie konto w wyniku ataku socjotechnicznego.
WF - Płace	System e-BANK	Błędy pracownika	Wykorzystanie przekazanych danych do logowania do systemu księgowego nieuprawnionej osobie.
WF - Płace	System księgowy	Uszkodzenie	Uszkodzenie systemu księgowego w wyniku którego program działa niepoprawnie.
WF - Płace	Token	Błędy pracownika	Pozostawienie urządzenia wraz z danym do logowania.
WF - Płace	Token	Błędy pracownika	Udostępnienie urządzenia nieuprawnionej osobie.
WF - Płace	Token	Uszkodzenie	Uszkodzenie urządzenia uniemożliwiające potwierdzenie przelewu.

Zakładka Edycja **procesu** umożliwia przypisanie do procesu.

## 6. Dodanie nowego ryzyka.

Po wybraniu przycisku 'Dodaj' pojawia się okno dodawania komórki organizacyjnej, komponentów, grupy podatności i ryzyk.

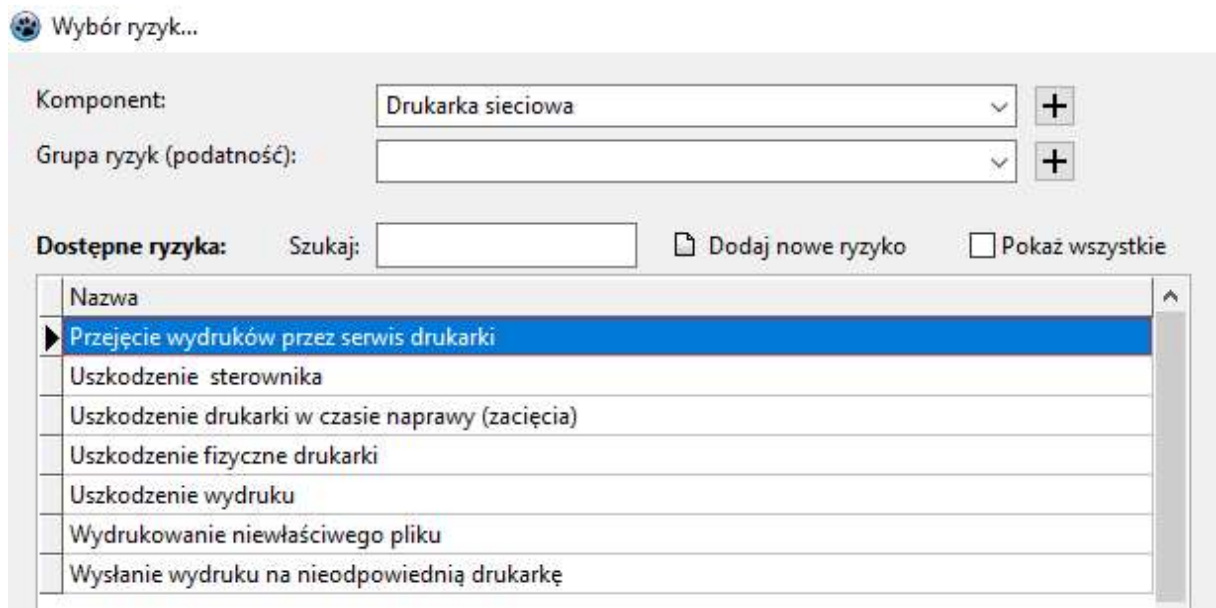



Wybranie istniejącego komponentu i grupy ryzyk umożliwia pole wyboru.

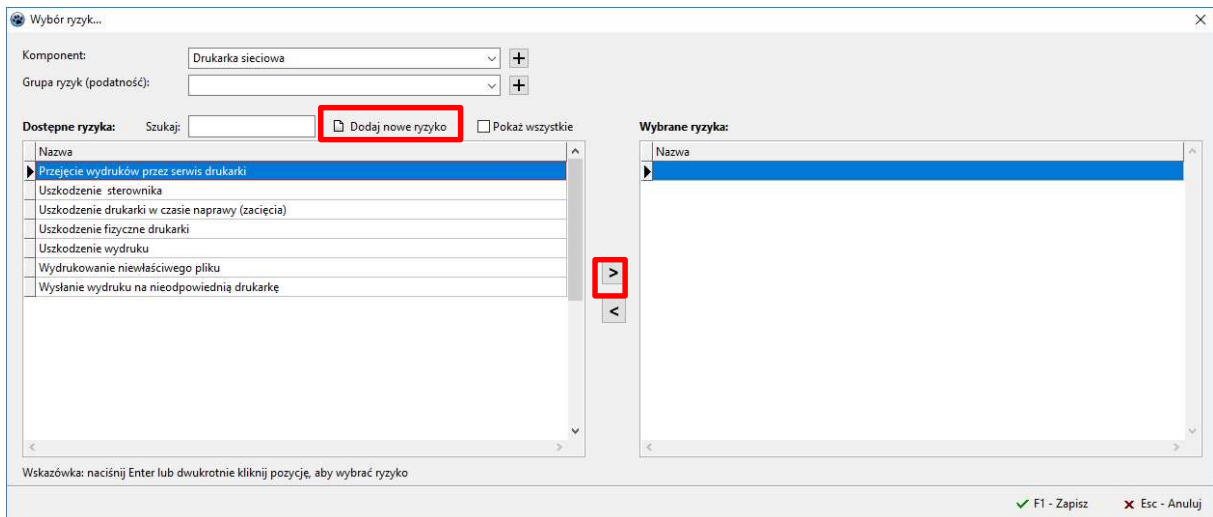


W przypadku dodania nowego komponentu lub grupy ryzyka należy kliknąć znak plusa.

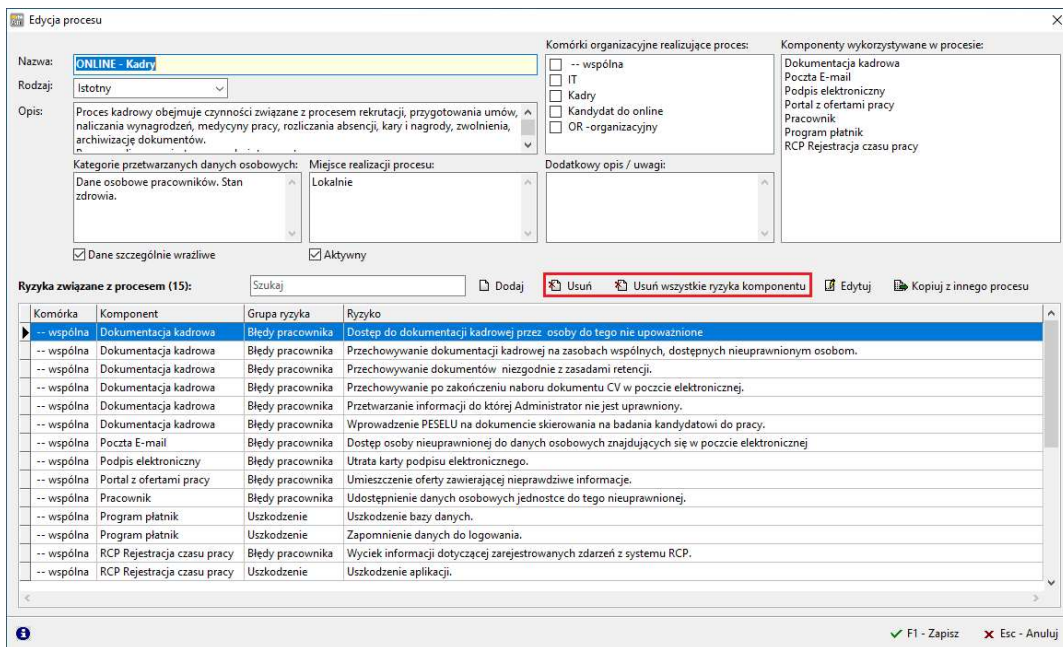
7. Wybranie istniejącego komponentu wyświetli przypisane do niego ryzyka.



Można wybrać dostępne ryzyka klikając na znak  lub dodać nowe ryzyko.



## Kasowanie ryzyk w procesie.

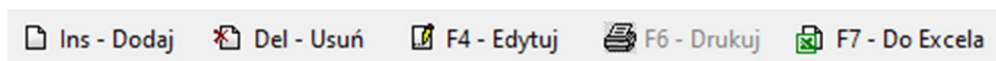


### 1. Przycisk 'Usuń' – usuwa podświetlone ryzyko.

Usuwanie wszystkich ryzyk z danego komponentu - w tym celu należy **'zaznaczyć komponent'**, którego ryzyka mają zostać usunięte i kliknąć **'Usuń wszystkie ryzyka z komponentu'**. W tym przypadku usuniętych zostanie 6 ryzyk dotyczących dokumentacji kadrowej.

## Edycja komponentu.

### 1. Panel zakładki komponenty.



**Ins – Dodaj** – umożliwia dodanie nowego komponentu.

**Del – Usuń** – umożliwia skasowanie wybranego komponentu.

**F4 – Edytuj** – pozwala na wprowadzenie zmian w komponentcie.



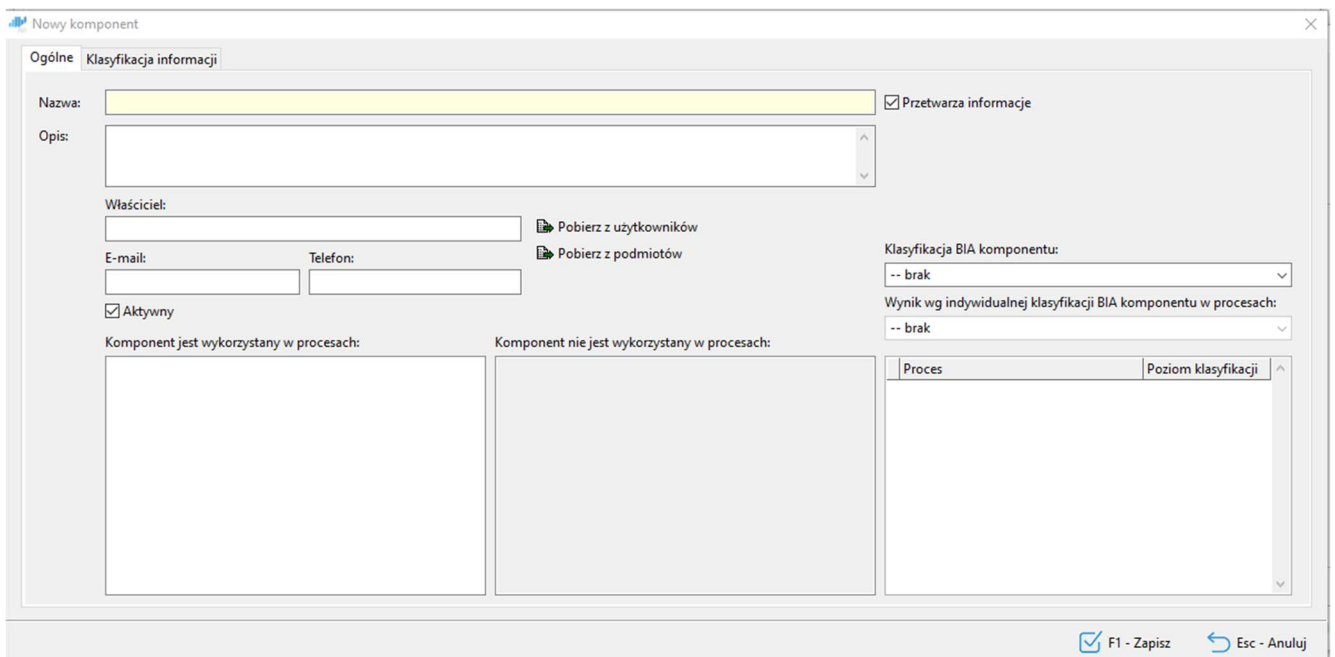
**F6 – Drukuj** – drukowanie nieaktywne na tym widoku

**F7 – Do Excella** – pozwala na eksport widocznych na ekranie komponentów do aplikacji Excel.

2. Widok komponentów zawiera kolumny:

- Nazwa - nazwa komponentu.
- Opis – opis komponentu.
- Wykorzystano – informuje czy komponent jest powiązany z procesem.
- Aktywny - informacja czy komponent zostanie uwzględniony w raporcie.

3. **Dodanie** nowego komponentu.

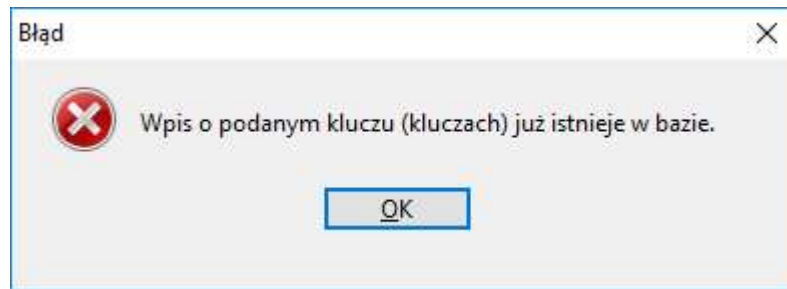


W celu dodania nowego komponentu wystarczy wypełnić pola tekstowe nazwa i opis.

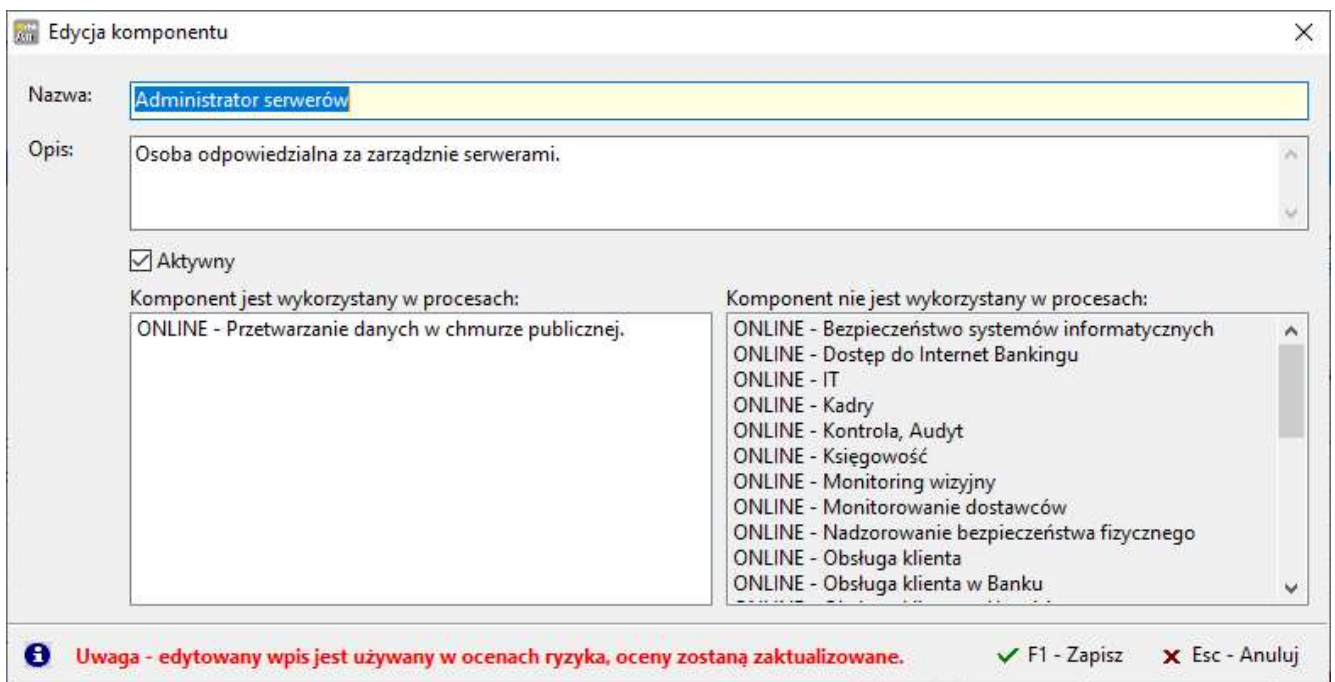
Dodatkowo istnieje możliwość:

- przypisania właściciela z jego danymi kontaktowymi,
- ustawienia aktywności komponentu (wykorzystywane w przypadku, gdy komponent został np. wycofany),
- przypisania klasyfikacji BIA dla komponentu w ramach procesu,
- przypisania klasyfikacji informacji w ramach procesu.

Program nie pozwoli na wprowadzenie dwóch komponentów o takiej samej nazwie.  
Wyświetli komunikat.

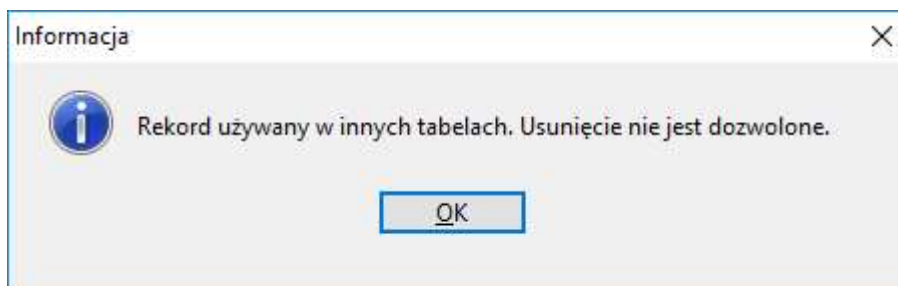


#### 4. Edycja komponentu pozwana na kontrolę powiązań komponentów z procesami.



#### 5. Kasowanie komponentu jest możliwe, jeżeli nie jest połączony z innymi procesami.

Aplikacja poinformuje o niedozwolonej funkcji.



Edycja ryzyka.

#### 1. Panel zakładki komponenty.

Ins - Dodaj   Del - Usuń   F4 - Edytuj   F6 - Drukuj   F7 - Do Excela

**Ins – Dodaj** – umożliwia dodanie nowego ryzyka.

**Del – Usuń** – umożliwia skasowanie wybranego ryzyka.

**F4 – Edytuj** – pozwala na wprowadzenie zmian w ryzykach.

**F6 – Drukuj** – pozwala na wydrukowanie widocznych na ekranie ryzyk.

**F7 – Do Excela** – funkcja nieaktywna w tym widoku.

2. Widok ryzyk zawiera kolumny:

- Nazwa - nazwa ryzyka.
- Opis – opis ryzyka.
- Aktywny - informacja czy ryzyko zostanie uwzględnione w raporcie.

3. Dodanie nowego ryzyka.

Istnieją dwie możliwości na dodanie nowego ryzyka. Wykorzystując zakładkę Ryzyka wpisujemy nazwę ryzyka oraz opis lub podczas zarządzania procesem można dodawać nowe ryzyka i wiązać je z komponentem i komórką organizacyjną.



Do wprowadzenia nowego ryzyka wystarczy wypełnienie pola **Nazwa**, pole Opis jest opcjonalne.

Filtrowanie ryzyk w zakładce ocena ryzyka.

1. Oceny ryzyka dokonuje się w zakładce 'Ocena ryzyka'.

Proces	Komórka	Komponent	Grupa ryzyka	Ryzyk	Ryzyko wstępne	Ryzyko końcowe	Ocena wykonana	Wykonana przez	Data przeglądu
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	Programista	Świadome działanie na niekorzyść firmy	Doc	3,0	4,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	Programista	Świadome działanie na niekorzyść firmy	Poz	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy administratora	BraJ	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy administratora	BraJ	3,0	4,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy administratora	BraJ	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy administratora	BraJ	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy administratora	Test	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy pracownika	Wpi	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy programisty	Blec	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy programisty	BraJ	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy programisty	NieJ	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy programisty	NieJ	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy programisty	Wpi	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy programisty	Wpi	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Błędy programisty	Wyl	3,0	4,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Cyberprzestępczość	NieJ	3,0	4,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Kadrowe	BraJ	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Zagrożenia zewnętrzne	Upa	2,0	3,0	Tak	Administrator	
ONLINE - Bezpieczeństwo systemów informatycznych	-- wspólna	System informatyczny	Zagrożenia zewnętrzne	Zak	2,0	3,0	Tak	Administrator	
ONLINE - Dostęp do Internet Bankingu	-- wspólna	Internet Banking	klient banku	BraJ	3,0	4,0	Tak	Administrator	
ONLINE - Dostęp do Internet Bankingu	-- wspólna	Internet Banking	klient banku	Udc	3,0	4,0	Tak	Administrator	
ONLINE - Dostęp do Internet Bankingu	-- wspólna	Internet Banking	klient banku	Utr	1,0	2,0	Tak	Administrator	
ONLINE - IT	-- wspólna	DHCP	Błędy administratora	Uru	3,0	2,0	Tak	Administrator	
ONLINE - IT	-- wspólna	DLP	Błędy administratora	NieJ	2,0	3,0	Tak	Administrator	
ONLINE - IT	-- wspólna	DLP	Błędy administratora	Udc	3,0	4,0	Tak	Administrator	
ONLINE - IT	-- wspólna	DNS	Błędy pracownika	DNE	2,0	2,0	Tak	Administrator	

## 2. Filtrowanie podstawowe.

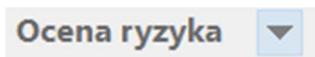
Ocena ryzyka | Proces: Wszystkie | Poziom ryzyka: Wszystkie | Przegląd: Wszystkie

Umożliwia wyświetlenie wszystkich ryzyk z:

- Procesu.
- Według poziomu ryzyka (akceptowalne i nieakceptowalne).
- Przegląd (wymagające przeglądu i z wykonanym przeglądem).

## 3. Filtrowanie rozszerzone.

Filtr rozszerzony uruchamia się za pomocą przycisku.



Proces: Wszystkie | Poziom ryzyka: Wszystkie | Przegląd: Wszystkie |  Tylko z KRI  
 Status: Wszystkie | Komponent: Wszystkie | Właściciel komp.:  
 Regulacja: Wszystkie | Grupa ryzyka: Wszystkie |  Z przekroczonym terminem realizacji planu postępowania  
 Komórka: Wszystkie | Inf. zarządca: Wszystkie |  Obligatoryjne (z blokadą usuwania)  
 Jednostka: Wszystkie | Plan zaawans.: Wszystkie |  Podczas edycji ustaw automatycznie 'Ocena wykonana'  
 Data: -- brak filtru | Ocena wykonana: |  Operacje zaawansowane

Aplikacja umożliwia filtrowanie w zakresie selekcji:

- Procesów – umożliwia wybranie ryzyk należących do jednego procesu.
- Statusu – umożliwia wybranie tylko tych ryzyk, których analiza została wykonana bądź niewykonana lub umożliwia wybór wszystkich ryzyk.
- Regulacji – umożliwia wybranie ryzyk przypisanych do regulacji.
- Komórki – umożliwia wybranie ryzyka przypisanego do komórki.
- Jednostki – jednostki organizacyjnej wprowadzonej do aplikacji.

- Daty – utworzenia, ostatniej aktualizacji oceny, wykonania przeglądu.
- Poziomu ryzyka – umożliwia wyświetlenie ryzyk nieakceptowalnych, akceptowalnych lub wszystkich ryzyk.
- Komponentu – umożliwia wybór pojedynczego komponentu.
- Grupa ryzyka – umożliwia wyświetlenie odpowiedniej grupy ryzyka.
- Inf. zarządczej – umożliwia przypisanie ryzyk do informacji zarządczej.
- Planu zaawansowania – wprowadzonych planów postępowania z ryzykiem.
- Osoby wykonującej – identyfikuje ryzyka wg osoby, która wykonała ocenę.
- Przeglądu – umożliwia wyświetlenie ryzyk wymagających przeglądu.
- Właściciela komponentu – identyfikuje ryzyka wg właścicieli komponentu.
- Z przekroczonym terminem realizacji planu postępowania.
- Obligatoryjne – z blokadą usuwania.
- Tylko KRI – identyfikuje ryzyka ze zdefiniowanym KRI.

## Ocena ryzyka.

**Proces:** a. ONLINE - Kadry Komórka: Kadry

**Komponent:** Dokumentacja kadrowa

**Grupa ryzyka (podatność):** Błędy pracownika

**Ryzyko:** Dostęp do dokumentacji kadrowej przez osoby do tego nie upoważnione

**Opis ryzyka:** Dostęp do dokumentacji nieupoważnionych pracowników lub osoby z zewnątrz.

**Prawdopodobieństwo wystąpienia:** b. 1 2 3 4 5 c.  **Ryzyko wstępne: 3,0** **Ryzyko końcowe: 2,0**

Skutki wystąpienia		1	2	3	4	5	Opis skutków
d. Finansowe:			2	3	4	5	Starata nie przekracza 10.000 zł.
Wizerunkowe:		1	2	3	4	5	Informacje ograniczone do wszystkich pracowników
Poufność:		1	2	3	4	5	Utracone informacje dotyczą jednego działu (zbioru)
Integralność:		1	2	3	4	5	Zagrozenie nie wpływa na utratę integralności
Dostępność:		1	2	3	4	5	Zagrozenie nie wpływa na utratę dostępności

**e.** Ocena ryzyka naruszenia praw lub wolności osób fizycznych: 1 2 3 4 5 Skutki ryzyka dla danych osobowych:

kradzież środków finansowych, nieuprawnione zawarcie zobowiązań, wyłączenie mediów, stres klienta,

**f.** Ocena dodatkowych atrybutów Opis mechanizmów:

**g.** Mechanizmy obniżające ryzyko: 1 2 3 4 5 Zasady organizacyjne, przeszkoleni pracownicy, wskazane miejsca w których mogą przebywać osoby

**h.** Plan postępowania z ryzykiem: Zaawansowany plan postępowania z ryzykiem Opis planu:

Oznacz ocenę jako wykonaną Ocena wykonana przez: Administrator j.  Ocena obligatoryjna  F1 - Zapisz  Esc - Anuluj

1. **W sekcji a** wyświetlane są informacje na temat ocenianego procesu oraz możliwość przypisania ryzyka innej komórce.
2. **W sekcji b** oceniane jest prawdopodobieństwo wystąpienia ocenianego ryzyka, zgodnie z przyjętą metodyką.

Wskazując kursorem na wartości liczbowe program podpowiada definicję danej wartości.



1	2	3	4	5
Takie zdarzenie nie miało miejsca.				

3. **W sekcji c** po określeniu wartości prawdopodobieństwa, skutków wystąpienia, utraty danych osobowych oraz mechanizmów obniżających ryzyko, program wylicza ryzyko wstępne (bez mechanizmów obniżających ryzyko) oraz ryzyko końcowe.
4. **Sekcja d** służy do oceny skutków wystąpienia danego zdarzenia. Opis skutków wyświetlany jest po prawej stronie.
5. **Sekcja e** służy do oceny ilości utraconych danych osobowych oraz wskazania skutków ryzyka dla danych osobowych.
6. **Sekcja f** służy do oceny dodatkowych atrybutów wskazanych w **Parametry->Definicje dodatkowych atrybutów**.

Skutki wystąpienia	1	2	3	4	5	Opis skutków
Detekcji	1	2	3	4	5	Zagrożenie zostanie wykryte w czasie 48h
Wpływ na inne procesy	1	2	3	4	5	Zagrożenie wpływa na procesy wspomagające
Zakres utraty DO	1	2	3	4	5	Tracimy dane pracowników i ich rodzin



 F1 - Zapisz   
  Esc - Anuluj

Przeprowadzenie oceny dodatkowych atrybutów sygnalizowane jest informacją na przycisku. W nawiasie wskazana jest liczba dokonanych ocen.

Ocena dodatkowych atrybutów (3)

7. **Sekcja g** służy do określenia mechanizmów, które wpływają na obniżenie ryzyka.



W przypadku wybrania wartości 3-5 aplikacja wymaga, aby dodany był opis zastosowanych mechanizmów.

8. **Sekcja h** służy do przygotowania planu postępowania z ryzykiem. W pierwszej zakładce wprowadza się opis.

Zakładka **zaawansowany plan postępowania z ryzykiem** służy do określenia szczegółów planu.

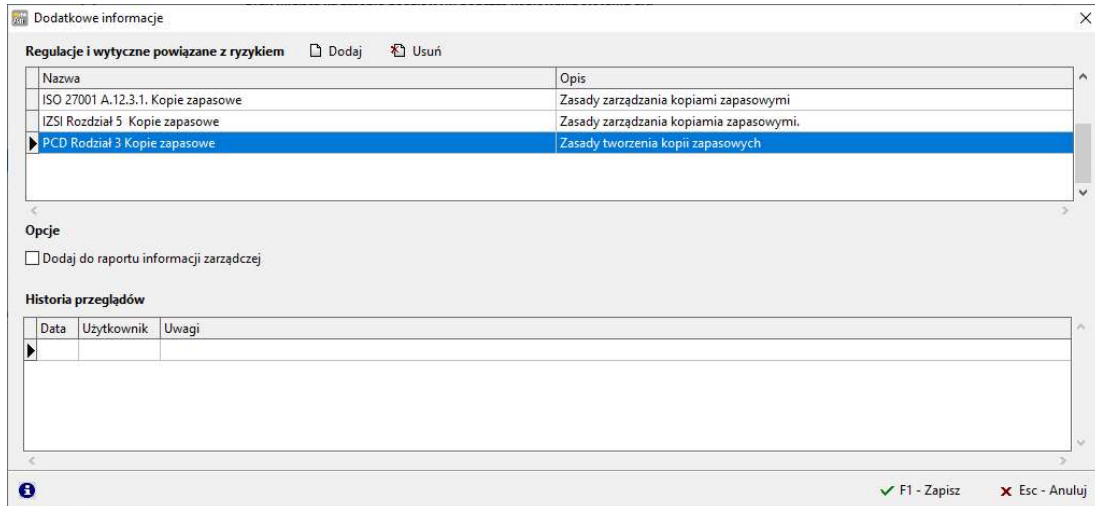


Plan postępowania należy wypełnić za każdym razem, gdy ryzyko osiągnie poziom nieakceptowalny.

Plan postępowania z ryzykiem	Zaawansowany plan postępowania z ryzykiem
Sposób realizacji:	Brak
Priorytet:	Niski
Osoba odpowiedzialna:	
Przewidywane koszty:	
Data realizacji:	27.03.2019

9. **Sekcja i** umożliwia:

- W 'Dodatkowych informacjach' przypisanie regulacji do ryzyka, po wcześniejszym ich zdefiniowaniu (Słowniki -> Regulacje / Wytyczne).
- W 'Dodatkowych informacjach' analizę wcześniej wykonanych przeglądów.
- Wykonanie przeglądu ryzyka.



The screenshot shows a window titled 'Dodatkowe informacje' with a sub-header 'Regulacje i wytyczne powiązane z ryzykiem'. It contains a table with two columns: 'Nazwa' and 'Opis'. The table lists three entries: 'ISO 27001 A.12.3.1. Kopie zapasowe', 'IZSI Rozdział 5 Kopie zapasowe', and 'PCD Rodział 3 Kopie zapasowe'. The third entry is selected. Below the table is an 'Opcje' section with a checkbox 'Dodaj do raportu informacji zarządczej'. At the bottom is a 'Historia przeglądów' section with a table with columns 'Data', 'Uzytkownik', and 'Uwagi'.

- Przypisanie ryzyka do raportu informacji zarządczej. Funkcja jest wykorzystywana w przypadku, gdy ryzyko ma pojawić się w raporcie „Raport informacji zarządczej”.
- Monitorowanie historii przeglądów.

2. .

## Raportowanie.

1. Obecnie na zakładce Raporty program pozwala na generowanie raportów oraz dokonanie przeglądu uprawnień.
2. Dostępne są raporty:
  - Pełen raport z oceny ryzyka,
  - Raport informacji zarządczej,
  - Raport dane osobowe DPIA,
  - Raport wg regulacji, wytycznych i atrybutów,
  - Raport KRI.



Raport informacji zarządczej będzie pusty do momentu przypisania ryzyka na zakładce „Dodatkowe informacje”.

3. Generując raport istnieje możliwość określenia:
  - tytułu raportu,
  - informacji o autorach raportu,
  - uwag,
  - procesów i komponentów, które mają znaleźć się w raporcie.

Raport z oceny ryzyk

Tytuł raportu:

Autorzy:

Uwagi:

Zachowane raporty roczne (do celów statystycznych):

Rok	Data utworzenia
2019	14.02.2020

Uwzględnij procesy:  Wszystkie

- Audyt bezpieczeństwa 2019
- Bank - Dostęp do Internet Bankingu
- Bank - Obsługa klienta
- Bank - Zespół monitoringu restrukturyzacji i win
- IT
- Kadry
- Kontrola, Audyt
- Księgowość
- Nadzorowanie firm zewnętrznych
- Obsługa klienta
- Obsługa płatności internetowych
- Obsługa strony internetowej
- Obsługa strony internetowej BIP
- Obsługa strony internetowej Facebook
- Obsługa wniosków
- Pozwolenie na ściąganie zwłok z zagranicy
- Projekty Unijne
- Prowadzenie ZFSS
- Rekrutacja
- Szkolenia bezrobotnych
- TFI - ocena nowego systemu do front office

Uwzględnij komponenty:  Wszystkie

- Administrator serwerów
- Administrator sieci
- BIP
- DHCP
- DLP
- DNS
- Dokumentacja audytowa - Raport w formie elektronicznej
- Dokumentacja audytowa - Raport w formie papierowej
- Dokumentacja elektroniczna (.doc .xls .ppt)
- Dokumentacja finansowa
- Dokumentacja kadrowa
- Dokumentacja kredytowa
- Dokumentacja projektów unijnych.
- Dokumentacja tradycyjna
- Dokumentacja ZFSS
- Dokumentacja ZUS, RCA, DRA
- Dostawca usług
- Drukarka sieciowa
- Dyspenser
- Elektroniczny system kontroli dostępu
- Firewall (Zapora sieciowa)

Tylko wybrane komórki:  Wszystkie

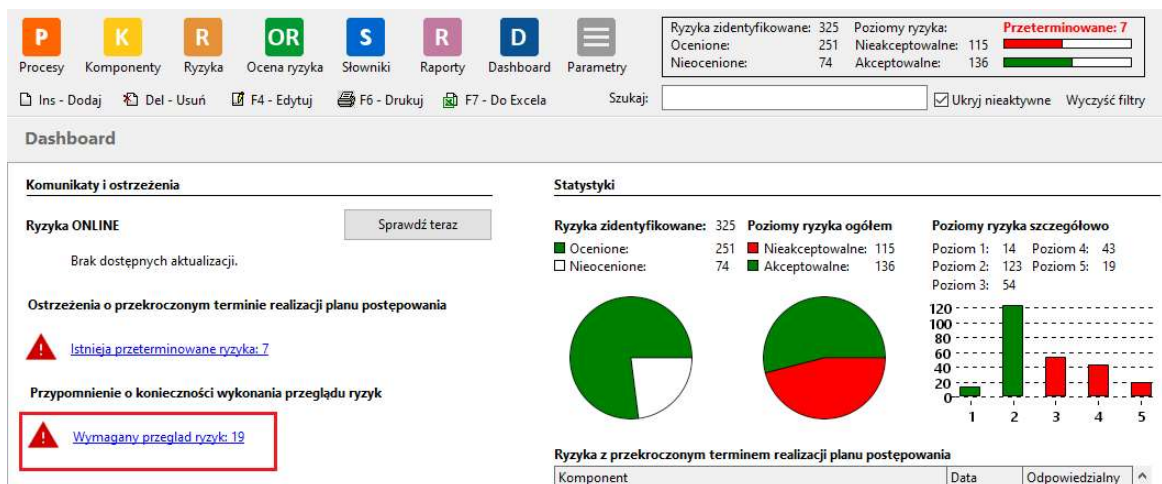
- IT - departament informatyki
- Kadry
- Księgowość
- OR - organizacyjny

F1 - Generuj raport  Esc - Anuluj

- Funkcja Zachowane raporty roczne (do celów statystycznych) – generuje się po przekazaniu raportu do najwyższego kierownictwa. Raport uwzględniający zmiany pomiędzy raportami zostanie wprowadzony w kolejnych wersjach.

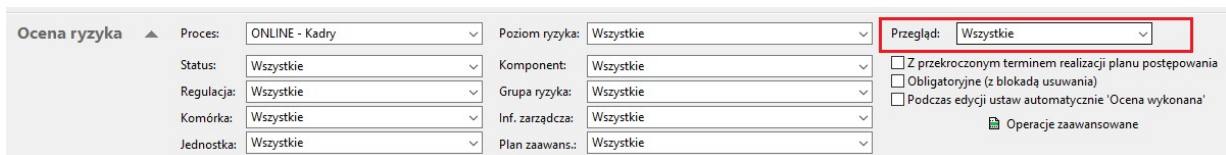
## Przegląd ryzyka.

- Ustawienie parametrów przeglądu opisane zostało w punkcie **Konfiguracja programu**.
- Program informuje o ryzykach, które wymagają przeglądu. Informacja ta jest dostępna na Dashboardzie.

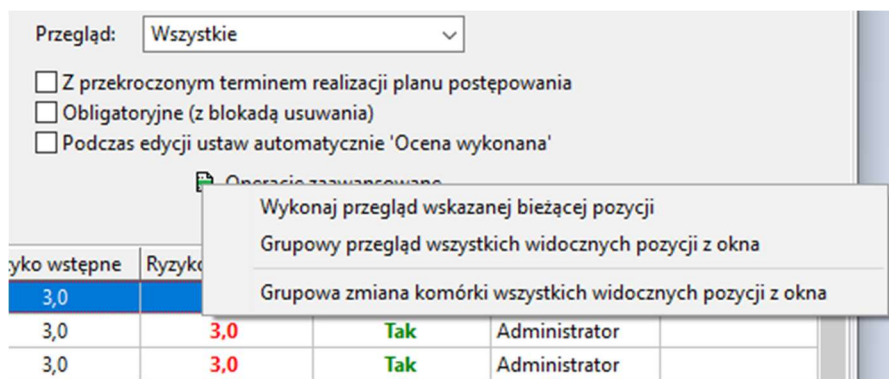




3. Za pomocą filtrów w **Ocenie ryzyka** możliwe jest wskazanie ryzyk wymagających przeglądu oraz ryzyk z wykonanym przeglądem.

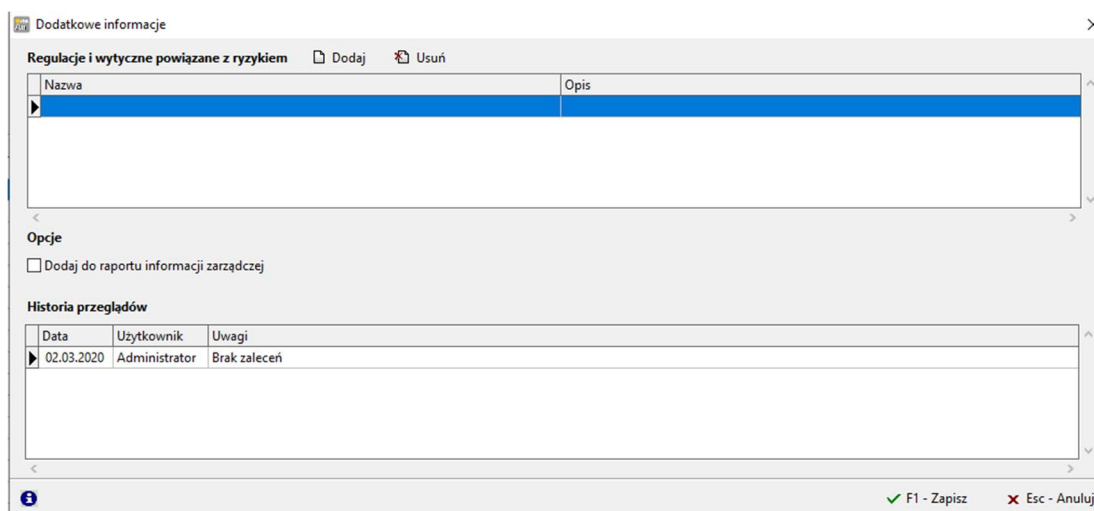


4. Program umożliwia dokonywanie pojedynczych przeglądów (zalecane) oraz dokonywanie przeglądów dla wyświetlanych grup. Można wyfiltrować dowolny grupę i dla niej przeprowadzić grupowy przegląd. Wybór grupowego przeglądu znajduje się pod przyciskiem 'Operacje zaawansowane'.



Ryzyko wstępne	Ryzyko			
3,0				
3,0	3,0	Tak	Administrator	
3,0	3,0	Tak	Administrator	

5. Informacja o przeglądzie jest widoczna na oknie informacji dodatkowych dla każdego ryzyka indywidualnie.



Data	Użytkownik	Uwagi
02.03.2020	Administrator	Brak zaleceń

## KRI – Jednostki miar Key Risk Indicators (kluczowe wskaźniki ryzyka).

1. Funkcja umożliwia wprowadzenie jednostek miar stosowanych podczas analiz kluczowych wskaźników ryzyka.
2. Wprowadzając nową jednostkę miar należy wypełnić nazwę miary w polu Symbol, opis oraz miejsce dziesiętne w liczbie.

Dodanie KRI do ryzyka.

2. KRI definiuje się podczas oceny ryzyka. W dolnej części okna znajduje się zakładka KRI.

3. Zakładka KRI umożliwi dodawanie nowego mechanizmu pomiarowego, usuwanie oraz edycję KRI.

Nowa definicja KRI

Nazwa:

Opis:

Częstotliwość pomiaru  
Miesięcznie W okresie od: Miesiąc: 1 Rok: 2022 do: Miesiąc: 12 Rok: 2050

Parametry pomiaru  
Jednostka miary:

Pożądana wartość pomiaru MNIJSZA lub RÓWNA wartości granicznej

Wartość graniczna:

Odchylenie, po którym występuje poziom ostrzegawczy:

Przykład:  
150  
100  
50  
0  
OK  
1 2 3 4

F1 - OK Esc - Anuluj

#### 4. Dodając nowy mechanizm pomiarowy definiuje się:

- Nazwę KRI.
- Opis.
- Częstotliwość pomiaru (roczna, półroczna, kwartalna, miesięczna).
- Jednostki miary (nowe jednostki definiuje się w menu Słowniki > KRI > Jednostki miar).
- Wybór mechanizmu pomiaru, pożądana wartość pomiaru **mniejsza lub równa** wartości granicznej.

Pożądana wartość pomiaru MNIJSZA lub RÓWNA wartości granicznej

Wartość graniczna:

Odchylenie, po którym występuje poziom ostrzegawczy:

Przykład:  
150  
100  
50  
0  
OK  
1 2 3 4

- Wybór mechanizmu pomiaru, pożądana wartość pomiaru **większa lub równa** wartości granicznej.

Pożądana wartość pomiaru WIĘKSZA lub RÓWNA wartości granicznej

Wartość graniczna:

Odchylenie, po którym występuje poziom ostrzegawczy:

Przykład:  
150  
100  
50  
0  
OK  
1 2 3 4

- Wybór mechanizmu pomiaru, pożądana wartość pomiaru **w przedziale od do**.

Pożądana wartość pomiaru POMIĘDZY wartościami granicznymi

Wartości w przedziale od:  do:

Odchylenie, po którym występuje poziom ostrzegawczy:

Przykład:  
150  
100  
50  
0  
OK  
1 2 3 4

## KRI – Pomiar.

1. Na otwarciu zakładki z pomiarami możemy filtrować KRI według potrzeb. Podstawowym filtrem jest wyświetlanie KRI wymagających uzupełnienia (Status Wymagające uzupełnienia).

KRI - pomiary

Proces: Wszystkie Stan: Wszystkie Status: Wszystkie Za okres od: 2021 do: 2023

KRI: Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy niż 30 minut. Pokaż wykres

Proces	Ryzyko	Nazwa KRI	Okres	Wartość por.	J.m.	Wartość pożądana	Stan	Data pomiaru od	Data wypełnienia	Wypełnione przez
Nadzorowanie be:	Brak możliwości wykrycia n	Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy	pólr. 202		szt.	<= 0		01.01.2024		
Nadzorowanie be:	Brak możliwości wykrycia n	Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy	pólr. 202		szt.	<= 0		01.07.2023		
Nadzorowanie be:	Brak możliwości wykrycia n	Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy	pólr. 202		szt.	<= 0		01.01.2023		
Nadzorowanie be:	Brak możliwości wykrycia n	Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy	pólr. 202		szt.	<= 0		01.07.2022		
Nadzorowanie be:	Brak możliwości wykrycia n	Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy	pólr. 202	0	szt.	<= 0	Normalny	01.01.2022	11.01.2022	Administrator
Nadzorowanie be:	Brak możliwości wykrycia n	Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy	pólr. 202	1	szt.	<= 0	Przekroczony	01.07.2021	11.01.2022	Administrator

2. Uzupełnienie pomiaru polega na wprowadzeniu wartości pomiaru w polu Zmierzona wartość oraz wprowadzeniu wyjaśnienia w polu Uwagi, w przypadku przekroczenia wartości normalnej.

Za okres: I półr. 2021

Zmierzona wartość: [input type="text"]

Jednostka: szt.

Pokaż definicję KRI

Pomiar wykonany

Uwagi: Temperatura wzrosła do 28 stopni i utrzymywała się przez 12 godzin. Zdarzenie spowodowane uszkodzeniem klimatyzatora.

Wykonany przez: Administrator, dnia 11.01.2022

F1 - Zapisz  Esc - Anuluj

## Raportowanie KRI.

W systemie przygotowany został szablon ryzyka, pozwalający na przygotowanie raportu dotyczącego utrzymywanych pomiarów KRI.

Raport pozwala na:

- wygenerowanie zestawienia z okresu czasu,
- zawarcie w raporcie stanów niezgodnych (przekroczonych),
- zawarcie w raporcie stanów ostrzegawczych,
- wybór KRI, które mają znaleźć się w raporcie,
- wybór procesów objętych KRI.

Raport KRI

Tytuł raportu: Raport KRI

Autorzy: Administrator

Uwagi:

Za okres: 01.01.2021 - 02.12.2022

Tylko stan przekroczony  Tylko stan ostrzegawczy

Uwzględnij KRI:  Wszystkie Uwzględnij procesy:  Wszystkie

Brak dostępu do Internetu przekraczający 1h. - Ana

Brak możliwości odtworzenia bazy danych na pods

Identyfikacja obcego urządzenia podłączonego do

BOK - Biuro obsługi klienta

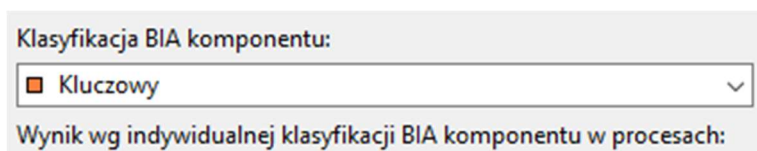
Księgowość - Obsługa finansowo - księgowo

Nadzorowanie bezpieczeństwa w Centrali - Bezpieczeństwo fizyczne dost

## Klasyfikacja komponentów.

Aplikacja umożliwia przypisanie każdemu komponentowi wagi zdefiniowanej w analizie BIA.

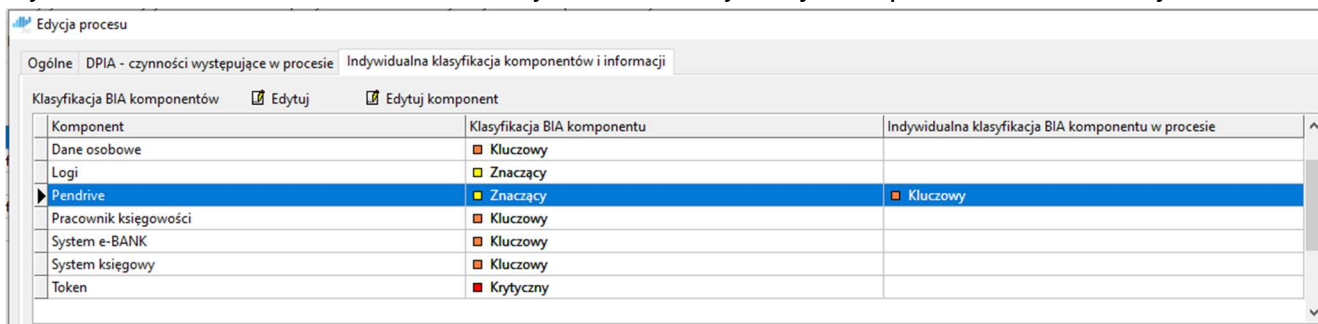
1. Analiza BIA. Program umożliwia przeprowadzenie analizy komponentu pod kątem wpływu jego utraty na organizację. Dla każdego zdefiniowanego komponentu można dokonać oceny.
2. Organizacja ma możliwość zdefiniowania atrybutów, które będą opisywały znaczenie komponentu. Standardowo są to:
  - Krytyczny,
  - Kluczowy,
  - Znaczący,
  - Wspomagający.
3. Przypisanie atrybutu komponentowi odbywa się na zakładce 'Komponenty'. W oknie 'Klasyfikacja BIA komponentu' wybiera się atrybut z listy.



## Klasyfikacja komponentu w kontekście procesu.

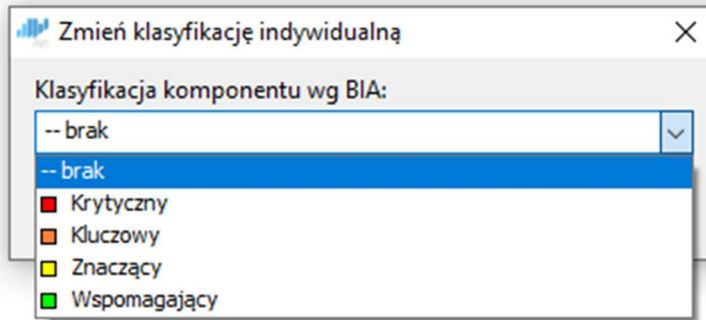
W przypadku, gdy główna klasyfikacja w kontekście danego procesu odbiega od przyjętej analizy istnieje możliwość indywidualnej oceny komponentu. Przykładowo w klasyfikacji nośnik wymienny został wskazany jako Wspomagający, ale w procesie archiwizowania danych właściciel procesu zmienił klasyfikację na Kluczowy.

1. Dodanie nowej oceny BIA dotyczącej komponentu w kontekście danego procesu można wykonać w 'Procesach', na zakładce 'Indywidualna klasyfikacja komponentów i informacji'.



Komponent	Klasyfikacja BIA komponentu	Indywidualna klasyfikacja BIA komponentu w procesie
Dane osobowe	<input checked="" type="checkbox"/> Kluczowy	
Logi	<input checked="" type="checkbox"/> Znaczący	
<b>Pendrive</b>	<input checked="" type="checkbox"/> Znaczący	<input checked="" type="checkbox"/> Kluczowy
Pracownik księgowości	<input checked="" type="checkbox"/> Kluczowy	
System e-BANK	<input checked="" type="checkbox"/> Kluczowy	
System księgowy	<input checked="" type="checkbox"/> Kluczowy	
Token	<input checked="" type="checkbox"/> Krytyczny	

2. Kolumna 'Klasyfikacja BIA komponentu' informuje jaką klasyfikację nadany miał komponent podczas klasyfikacji głównej.
3. Kolumna 'Indywidualna klasyfikacja BIA komponentu w procesie' informuje jakie klasyfikacje nadano w ramach oceny, w kontekście danego procesu.
4. Zmianę dokonujemy przyciskiem 'Edytuj', wybieramy odpowiedni atrybut.



5. Z tego okna można też edytować klasyfikację główną komponentu, w tym celu proszę kliknąć 'Edytuj komponent'

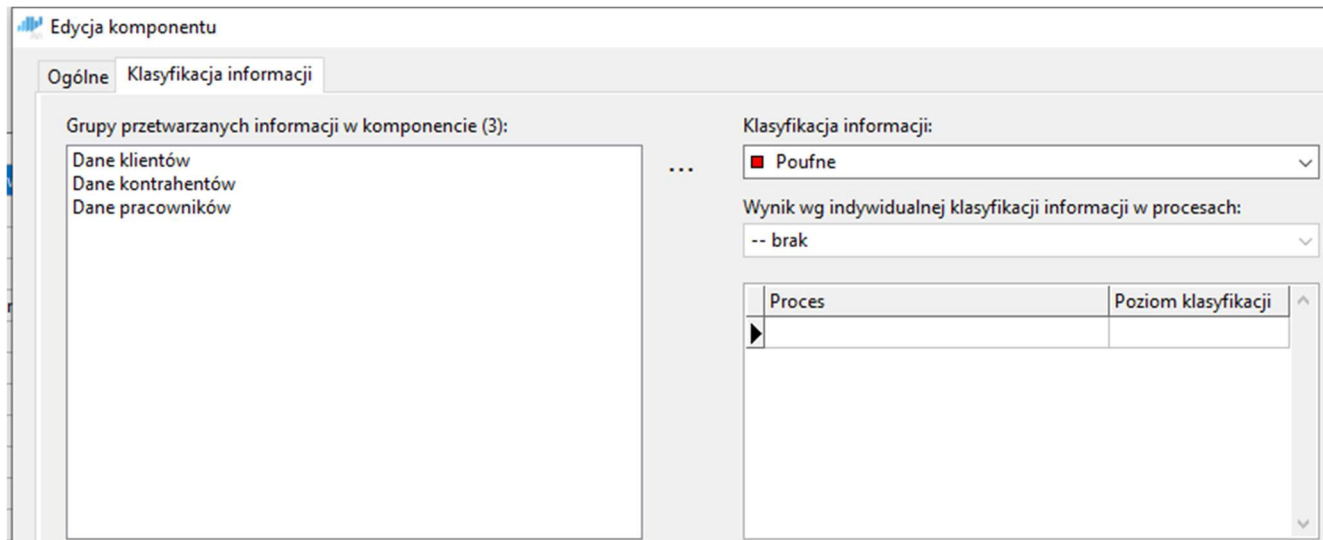
### Klasyfikacja informacji.

Program umożliwia klasyfikację informacji w kontekście przetwarzania jej na danym komponentcie. Analizę wykonuje się analogicznie, jak w przypadku klasyfikacji BIA. W programie dostępne są atrybuty:

- Poufne,
- Wewnętrzne,
- Publiczne,
- Niechronione.

Program umożliwia zmianę atrybutów na własne.

1. Aby dokonać klasyfikacji informacji przetwarzanej na komponentcie wchodzimy do zakładki 'Komponenty'.
2. Wybieramy komponent, na którym chcemy dokonać klasyfikacji.
3. Przechodzimy na zakładkę 'Klasyfikacja informacji'. W oknie grupy przetwarzanych informacji w komponentcie widzimy jaki zakres informacji przetwarzany jest na komponentcie i na ich podstawie dokonujemy klasyfikacji, wybierając w dostępnych opcjach odpowiednią klasyfikację.



4. Okno to zapewnia również dostęp do informacji o indywidualnych klasyfikacjach informacji zależnych od kontekstu procesu.

Klasyfikacja informacji w kontekście procesu.

Klasyfikacja informacji może zależeć od kontekstu, w którym jest wykorzystywana np. informacje o pracownikach na serwerze HR mogą być uznane za dane ściśle tajne, ale w aplikacji do monitorowania dostępu do budynku mogą mieć niższy poziom klasyfikacji, ponieważ są potrzebne tylko do autoryzacji wejścia. Różne komponenty systemu mogą wymagać różnych poziomów ochrony tej samej informacji, w zależności od jej roli i stopnia wrażliwości w danym kontekście.

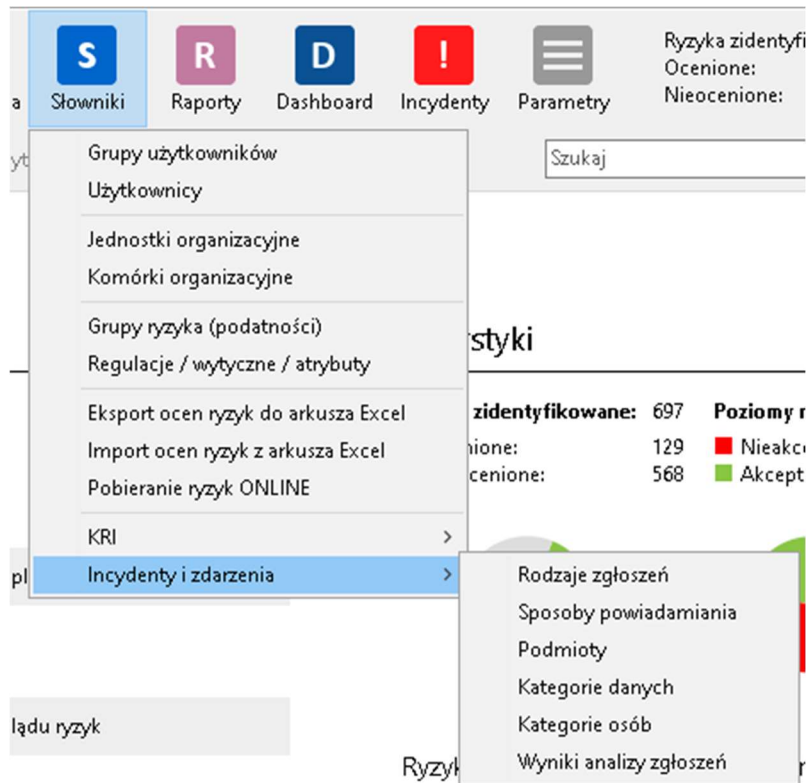
Analiza w kontekście informacji wykonywana jest analogicznie do analizy BIA.

- a) uruchomiony AnRisk jest dostępny zdalnie, port 3050 (np. za pomocą aplikacji telnet).

## Zarządzanie incydentami

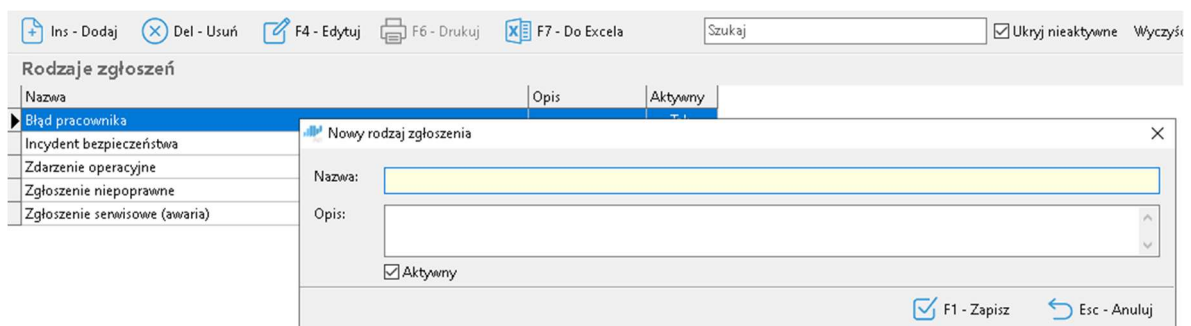
Konfiguracja.

1. Dostęp do ustawień możliwy jest w zakładce Słowniki.



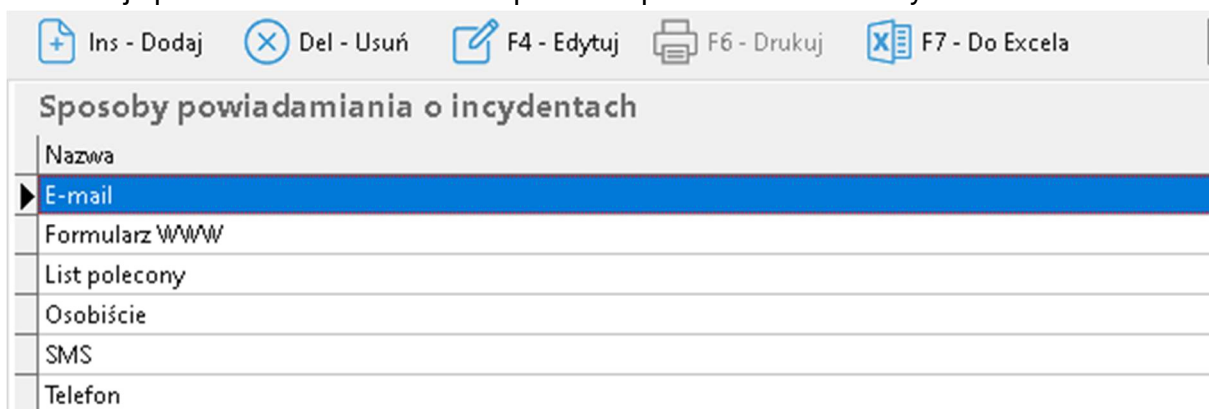
## 2. Rodzaje zgłoszeń.

Na tej zakładce administrator może zdefiniować własne rodzaje zgłoszeń. Funkcja ta pozwala na dostosowanie funkcji zarządzania incydentami zgodnie z obowiązującymi zasadami.



## 3. Sposoby powiadamiania.

Funkcja pozwala na zdefiniowanie sposobów powiadamiania o incydencie.



## 4. Podmioty.



Funkcja pozwala na dodanie listy podmiotów, które uczestniczą w procesach firmy oraz podmiotów, którym zgłasza się incydenty.

Nowy podmiot
✕

Nazwa:

NIP:

Adres:

Ulica:

Nr lokalu:

Miasto:

Kod pocztowy:

Kraj:

Dane kontaktowe

Tel. 1:

Tel. 2:

E-mail:

WWW:

Osoba kontaktowa:

Opis:

Aktywny

F1 - Zapisz    ↶ Esc - Anuluj

## 5. Kategorie danych.

Ta funkcja pozwala na zdefiniowanie kategorii danych osobowych przetwarzanych w firmie.

Kategorie danych			
Nazwa	Opis	Dane szczególne / art. 10 RODO?	Aktywna
Adres e-mail			Tak
Adres zamieszkania lub pobytu			Tak
Dane dotyczące zarobków i/lub posiadanego majątku			Tak
Data urodzenia			Tak
Imiona rodziców			Tak
Nazwa użytkownika i/lub hasło			Tak
Nazwiska i imiona			Tak
Nazwisko rodowe matki			Tak
Numer ewidencyjny PESEL			Tak
Numer rachunku bankowego			Tak
Numer telefonu			Tak
Seria i numer dowodu osobistego			Tak
Wizerunek			Tak
Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej		Tak	Tak
Dane dotyczące czynów zabronionych		Tak	Tak
Dane dotyczące seksualności lub orientacji seksualnej		Tak	Tak
Dane dotyczące wyroków skazujących		Tak	Tak
Dane dotyczące zdrowia		Tak	Tak
▶ Dane genetyczne		Tak	Tak
Dane o pochodzeniu rasowym lub etnicznym		Tak	Tak
Dane o poglądach politycznych		Tak	Tak
Dane o przekonaniach religijnych lub światopoglądowych		Tak	Tak
Dane o przynależności do związków zawodowych		Tak	Tak

## 6. Kategorie osób.

Funkcja programu wykorzystywana jest do zdefiniowania kategorii danych osobowych przetwarzanych w firmie.

Nazwa	Opis	Aktywna
Dzieci		Tak
Klienci (obecni i potencjalni)		Tak
Klienci podmiotów publicznych		Tak
Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)		Tak
Pacjenci		Tak
Pracownicy		Tak
Służby mundurowe (np. wojsko, policja)		Tak
Studenci		Tak
Subskrybenci		Tak
Uczniowie		Tak
Użytkownicy		Tak

## 7. Wyniki analizy zgłoszeń.

Program umożliwia budowanie własnych progów oceny incydentu. W przypadku wprowadzania zmian należy zdefiniować zasadę zgłaszania naruszenia danych osobowych do UODO.

L.p.	Nazwa	Opis	Kolor	UODO?	Aktywny
0	Akceptowalny		<span style="color: green;">■</span>		Tak
1	Niski		<span style="color: gray;">■</span>		Tak
2	Średni		<span style="color: yellow;">■</span>	Tak	Tak
3	Wysoki		<span style="color: red;">■</span>	Tak	Tak

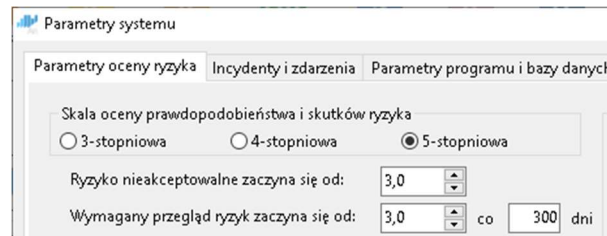
## Rejestracja incydentu.

### 1. Po otwarciu zakładki Incydynty wchodzimy w rejestr incydentów.

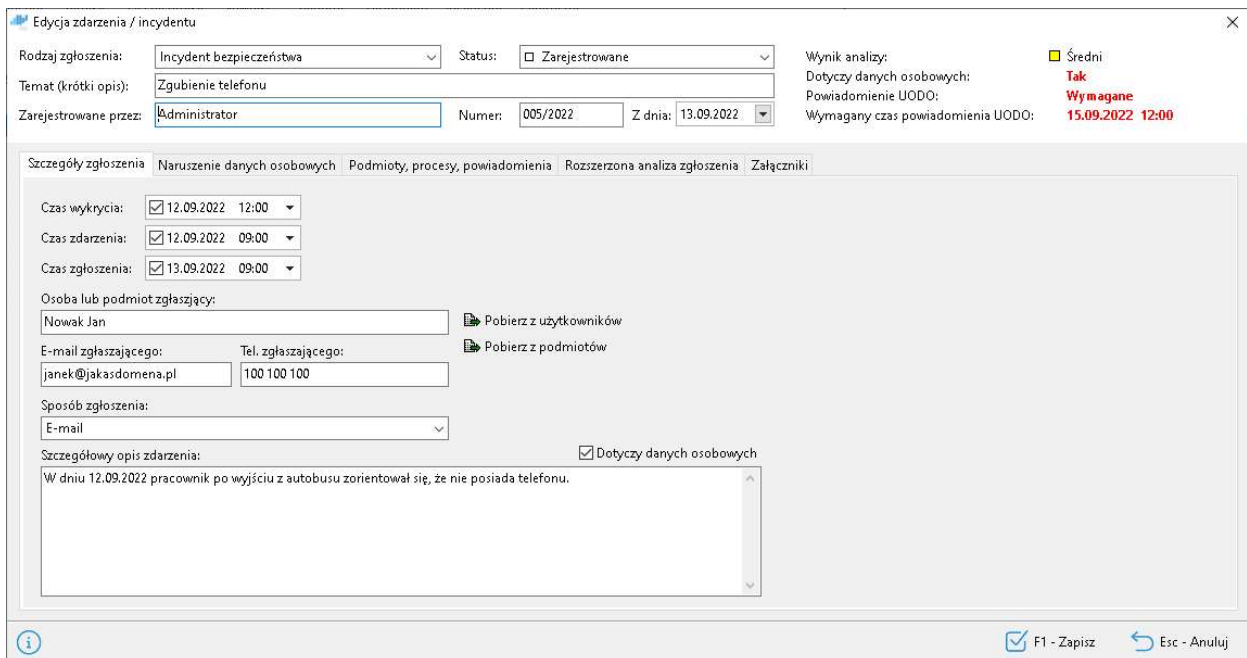
Data rejestracji	Numer	Tytuł zgłoszenia	Rodzaj zgłoszenia	Status	Użytkownik rejestrujący	Dane osobowe?
13.09.2022	005/2022	Zgubienie telefonu	Incident bezpieczeństwa	Zarejestrowane	Administrator	Tak
04.08.2022	004/2022	Uszkodzenie nośnika - utrata plików	Zgłoszenie serwisowe (awaria)	Zarejestrowane	Administrator	Nie
04.08.2022	003/2022	Router restartuje się - brak Internetu	Zgłoszenie serwisowe (awaria)	Zarejestrowane	Administrator	Nie
27.07.2022	002/2022	Kradzież dokumentacji	Błąd pracownika	Odrzucone	Administrator	Tak
12.07.2022	001/2022	Zatopienie telefonu	Błąd pracownika	Odrzucone	Administrator	Nie
07.07.2022	113	Zgubienie telefonu komórkowego	Błąd pracownika	Zarejestrowane	Administrator	Tak
05.07.2022	112	Nie działa drukarka (laser na korytarzu)	Zgłoszenie serwisowe (awaria)	Zakończzone	Administrator	Nie
05.07.2022	111	Wysłanie wiadomości zawierającej dane osobowe pod niewłaściwy adres	Incident bezpieczeństwa	Zarejestrowane	Administrator	Tak
04.07.2022	114	Zagubiony pendrive	Zdarzenie operacyjne	W realizacji	Administrator	Tak

### 2. Na zakładce szczegóły zgłoszenia zgłaszający definiuje:

- Rodzaj zgłoszenia.
- Status.
- Temat (krótki opis).
- Informację o osobie rejestrującej zdarzenie.
- Numer zgłoszenia (system umożliwia automatyczną numerację oraz numerację ręczną) zmiany definiuje się w Parametrach programu na zakładce Incydynty i zdarzenia.



- Czas wykrycia zdarzenia oraz zgłoszenia.
- Informację o osobie lub podmiocie zgłaszającym (można wpisać ręcznie lub pobrać z bazy użytkowników i podmiotów).
- Adres e-mail oraz telefon zgłaszającego.
- Szczegółowy opis zdarzenia.
- Checkbox dane osobowe wykorzystywany w przypadku, gdy zdarzenie dotyczy danych osobowych, zaznaczenie dodaje zakładkę Naruszenie danych osobowych.



### 3. Naruszenie danych osobowych.

Dostęp do tej funkcji jest możliwy po zaznaczeniu na zakładce szczegóły zgłoszenia checkbox'a Dotyczy danych osobowych.

Na tej zakładce wprowadzamy informacje o:

- Liczbie osób, których dotyczy zdarzenie,
- Liczba wpisów, które dotyczą jednej osoby,
- Kategorie danych,
- Kategorie osób,
- Dane szczególnych kategorii,
- Oraz informacje o analizie incydentu pod kątem naruszenia praw lub wolności.

Edycja zdarzenia / incydentu

Rodzaj zgłoszenia: Incyident bezpieczeństwa Status:  Zarejestrowane

Temat (krótki opis): Zgubienie telefonu

Zarejestrowane przez: Administrator Numer: 005/2022 Z dnia: 13.09.2022

Wynik analizy: ■ Średni  
Dotyczy danych osobowych: **Tak**  
Powiadomienie UODO: **Wymagane**  
Wymagany czas powiadomienia UODO: 15.09.2022 12:00

Szczegóły zgłoszenia | Naruszenie danych osobowych | Podmioty, procesy, powiadomienia | Rozszerzona analiza zgłoszenia | Załączniki

Liczba osób, których dotyczy zdarzenie: 500  
Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie: 5

Kategorie danych:  Adres e-mail  
 Adres zamieszkania lub pobytu  
 Dane dotyczące zarobków i/lub posiadanego majątku  
 Data urodzenia  
 Imiona rodziców  
 Nazwa użytkownika i/lub hasło  
 Nazwiska i imiona

Kategorie osób:  Dzieci  
 Klienci (obecni i potencjalni)  
 Klienci podmiotów publicznych  
 Osoby o szczególnych potrzebach (np. osoby starsze, niepełnospr  
 Pacjenci  
 Pracownicy  
 Służby mundurowe (np. wojsko, policja)

Inne niż powyższe:

Inne niż powyższe: członkowie rodzin

Dane szczególnych kategorii oraz dane, o których mowa w art.10 RODO:  Dane biometryczne w celu jednoznacznego zidentyfikowania os  
 Dane dotyczące czynów zabronionych  
 Dane dotyczące seksualności lub orientacji seksualnej  
 Dane dotyczące wyroków skazujących  
 Dane dotyczące zdrowia  
 Dane genetyczne  
 Dane o pochodzeniu rasowym lub etnicznym

Analiza incydentu pod kątem naruszenia praw lub wolności:

F1 - Zapisz Esc - Anuluj

#### 4. Podmioty, procesy, powiadomienia.

Zakładka służy do powiązania incydentu z procesami, komponentami oraz do rejestrowania strat. Aby dodać komponenty lub podmioty należy wybrać ikonę ... aby wybrać z listy odpowiednie zasoby.

Edycja zdarzenia / incydentu

Rodzaj zgłoszenia: Incyident bezpieczeństwa Status:  Zarejestrowane

Temat (krótki opis): Zgubienie telefonu

Zarejestrowane przez: Administrator Numer: 005/2022 Z dnia: 13.09.2022

Wynik analizy: ■ Średni  
Dotyczy danych osobowych: **Tak**  
Powiadomienie UODO: **Wymagane**  
Wymagany czas powiadomienia UODO: 15.09.2022 12:00

Szczegóły zgłoszenia | Naruszenie danych osobowych | Podmioty, procesy, powiadomienia | Rozszerzona analiza zgłoszenia | Załączniki

Powiązane komponenty: Smartfon ... Powiązane podmioty: ...  Zdarzenie objęte SLA

Analiza wpływu na procesy    Strata potencjalna: 30 000,00 Strata rzeczywista: 101,00

Data	Użytkownik	Proces	Strata potencjalna	Strata rzeczywista	Przerwa od	Przerwa do	Ile minut	Dotkliwość [0-10]
23.09.2022	Administrator	BOK	10 000,00	100,00				0
23.09.2022	Administrator	Marketing	20 000,00	1,00				0

Powiadomienia

Data	Użytkownik	Podmiot	Data powiadam.	Godz. powiadam.	Sposób	Uwagi	UODO?

F1 - Zapisz Esc - Anuluj

#### 5. Analiza wpływu na procesy.

Zakładka służy do określenia strat potencjalnych oraz strat rzeczywistych oraz określenie zakłócenia działania procesów w tym objętych umowami SLA.

Nowa analiza wpływu na proces

Proces: Marketing

Opis wpływu: Brak kontaktów z klientami

Wartość strat potencjalnych (najgorszy scenariusz dla skutków): 100 000,00

Wartość strat rzeczywistych (udokumentowanych):

W wyniku zdarzenia proces został przerwany lub poważnie zakłócony

Przerwa wystąpiła od: 23.09.2022 00:00 do: 23.09.2022 00:00

[poziom znikomy] Dotkliwość zdarzenia: 3 [poziom krytyczny]

F1 - OK Esc - Anuluj