Competence in Security
Information & Systems

Instrukcja obsługi

IMNS RISK MATRIX

Wersja 2.09

v.2.09

Data: 29.01.2024

Spis treści

Wprowadzenie.

Dziękujemy, że wybraliście Państwo naszą aplikację do zarządzania ryzykiem w Waszej firmie.

Dokument jest przewodnikiem po aplikacji, pozwalającym samodzielnie zainstalować oraz przeprowadzić analizę ryzyka.

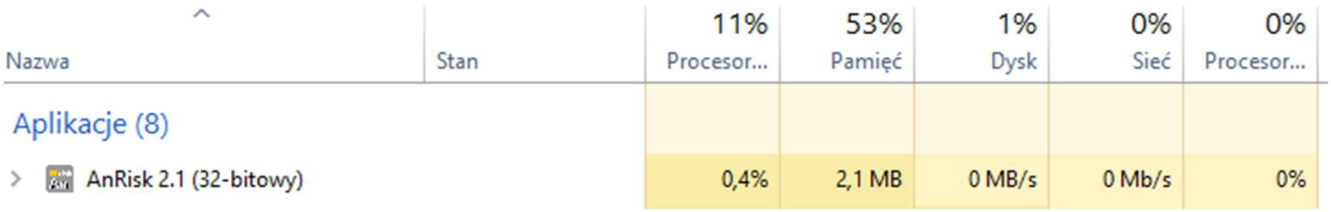
Administrator

1) Wymagania.

Do poprawnego działania aplikacji AnRisk wymagany jest aktualny, wspierany przez producenta system operacyjny Windows. Wersja 2.x nie wymaga instalacji klienta, ma ona formę portable. Należy zainstalować serwer bazy danych Firebird. Wszystkie niezbędne składniki do działania znajdują się w przygotowanych katalogach. W celu realizacji funkcji import/export bazy danych niezbędny jest aktualny, wspierany przez producenta program Excel.

Wymagania klienta		
System	Wspierany i aktualny system Windows.	Windows 10, 11
Miejsce na dysku	20	MB
Procesor i RAM	Brak specjalnych wymagań	n.d.
Oprogramowanie dodatkowe	Excel	Na jednej stacji do importu wzorców ryzyka.
Dostęp do Internetu	TAK	Tylko na stacji pobierającej ryzyka online.

Maksymalne obciążenie aplikacji nie przekracza 2% procesora i 10 MB RAM-u.
Średnie obciążenie obserwowane w programie to 0,5% i 4 MB RAM-u.



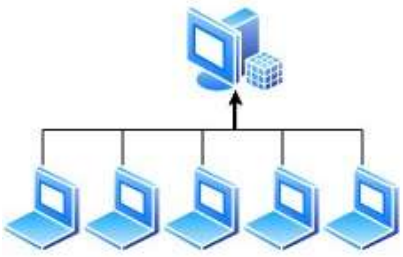
Wymagania serwera		
System	Wspierany i aktualny system	Windows 10, Windows Server, Linux, MAC
Miejsce na dysku	Aplikacja serwera Firebird	50 MB
	Baza 50 ryzyk	6 MB
	Baza 500 ryzyk	8 MB
	Baza 650 ryzyk	8.1 MB
Procesor i RAM	Brak specjalnych wymagań	n.d.
Dostęp do Internetu	Nie jest wymagany	n.d.

Bezpieczeństwo!

Z powodu wrażliwych informacji znajdujących się w programie, zalecamy przechowywanie kopii na nośnikach szyfrowanych**.**

Architektura

Program posiada klasyczną architekturę klient - serwer.



Istnieje możliwość pracy jednostanowiskowej. W takiej konfiguracji klient i serwer zainstalowane są na tej samej stacji lub serwerze.

Zaleca się umieszczenie aplikacji dostępowej na udziale sieciowym, co ułatwia proces aktualizacji aplikacji.

2) Instalacja

Instalacja realizowana jest w dwóch etapach. Etap 1 to instalacja serwera i bazy. Realizuje się go na urządzeniu, które będzie miało rolę dostępnego w sieci lokalnej komponentu. Etap 2 realizuje się na stacji roboczej lub na zasobie sieciowym, dostępnym dla osób odpowiedzialnych za realizację ryzyk.

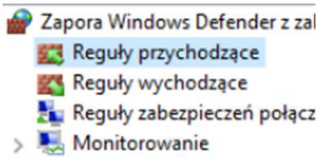
Etap 1. Instalacja serwera Firebird.

1. Ze strony https://firebirdsql.org/en/firebird-3-0/ pobieramy serwer 32 lub 64 bitowy (wersja 3.0.7 x64 znajduje się w katalogu Etap1).

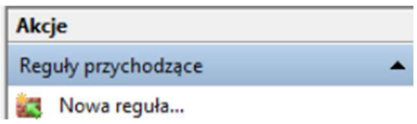
Win64			
64-bit Kits			
October 20, 2020	Firebird-3.0.7.33374_1_x64.exe	9 MB	Windows executable installer, recommended for first-time users

2. Instalujemy serwer na **standardowych** ustawieniach (nie są wymagane dodatkowe komponenty).
    1. W czasie instalacji ustawiamy **własne hasło** do bazy SYSDBA.

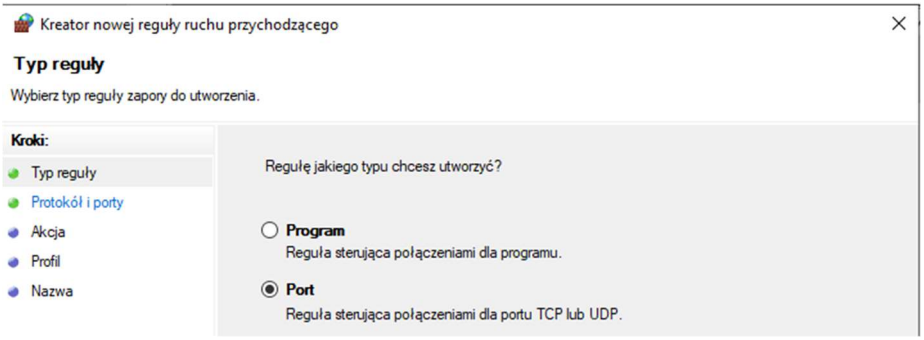
3. Odblokowujemy port **3050 tcp.**
    1. Uruchamiamy zaporę Windows i wchodzimy w **Reguły przychodzące.**



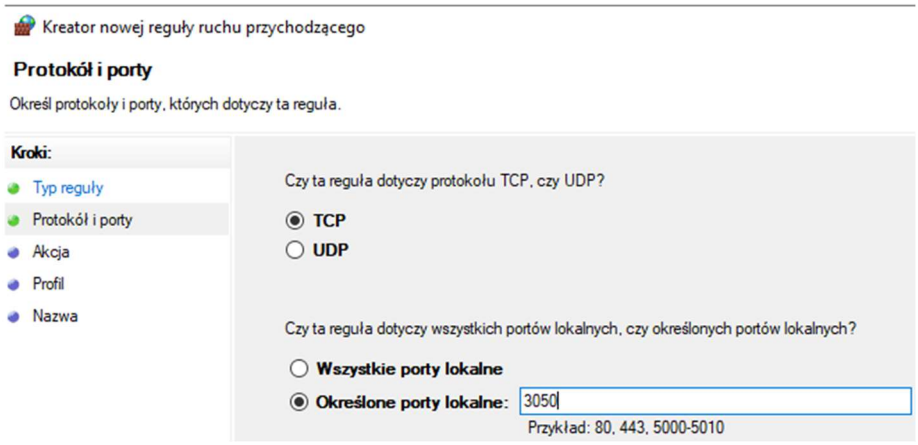
    2. Po prawej stronie wybieramy **Nowa reguła.**



3. W kreatorze reguły wybieramy **Port.**



4. Wpisujemy port 3050 i przypisujemy dowolną nazwę dla reguły.



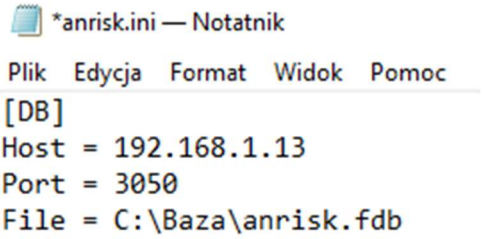
4. Zaleca się wykonać test połączenia ze stacji roboczej do serwera za pomocą telnetu, aby sprawdzić, czy port jest otwarty.
5. Zatrzymujemy usługę **Firebird Server – DefaultInstance.**
6. Kopiujemy plik **seciurity3.fdb** do katalogu, w którym zainstalował się serwer (C:\Program Files\Firebird\Firebird_3_0 **lub** Program Files (x86).
7. **Tworzymy katalog,** w którym będzie znajdowała się baza AnRisk (np. C:\baza). Katalog z plikiem bazy danych musi być umieszczony na lokalnym dysku serwera, nie może być to np. zmapowany udział sieciowy.
8. Plik **ANRISK.FDB** kopiujemy do przygotowanego w punkcie 7 katalogu.
9. Zalecenie: Proszę zapewnić **kopię** zapasową katalogu z bazą danych.
10. Uruchamiamy usługę **Firebird Server – DefaultInstance.**

Etap 2 – wykonywany jest w katalogu, w którym znajduje się program AnRisk.

1. Katalog **etap 2** zawiera wszystkie pliki niezbędne do działania aplikacji AnRisk. Należy umieścić je w katalogu sieciowym lub na dysku lokalnym.
   Zaletą użycia katalogu sieciowego jest przeprowadzanie aktualizacji programu w jednym miejscu.

2. Edytujemy plik **anrisk.ini** wprowadzając:

a. HOST = Adres IP serwera z zainstalowaną bazą,
b. Port = 3050,
c. File = Ścieżka do pliku na serwerze, w którym znajduje się baza.



Jeżeli program ma działać na tym samym komputerze, gdzie baza danych proszę ustawić adres IP na 127.0.0.1.

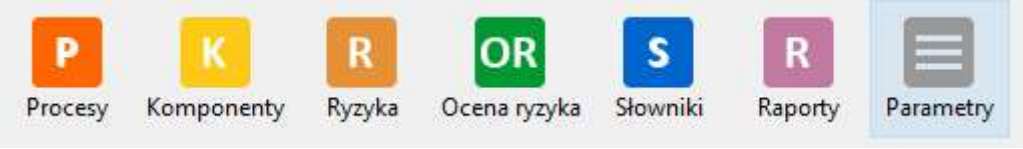
3) Logowanie.

Pierwsze logowanie do programu należy przeprowadzić na koncie ADMIN, tymczasowe hasło jest demo.

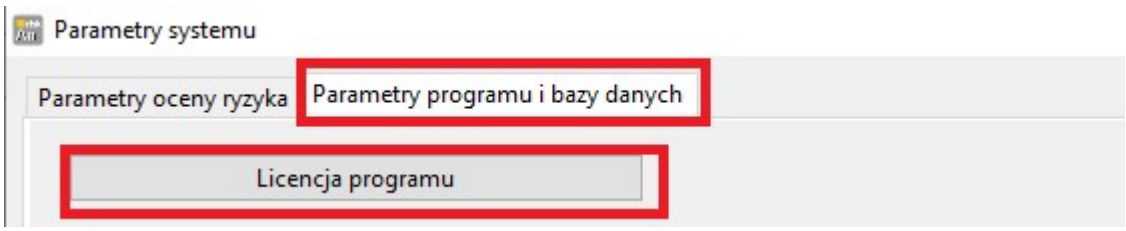
Należy zmienić hasło podczas pierwszego logowania.

4) Konfiguracja programu.

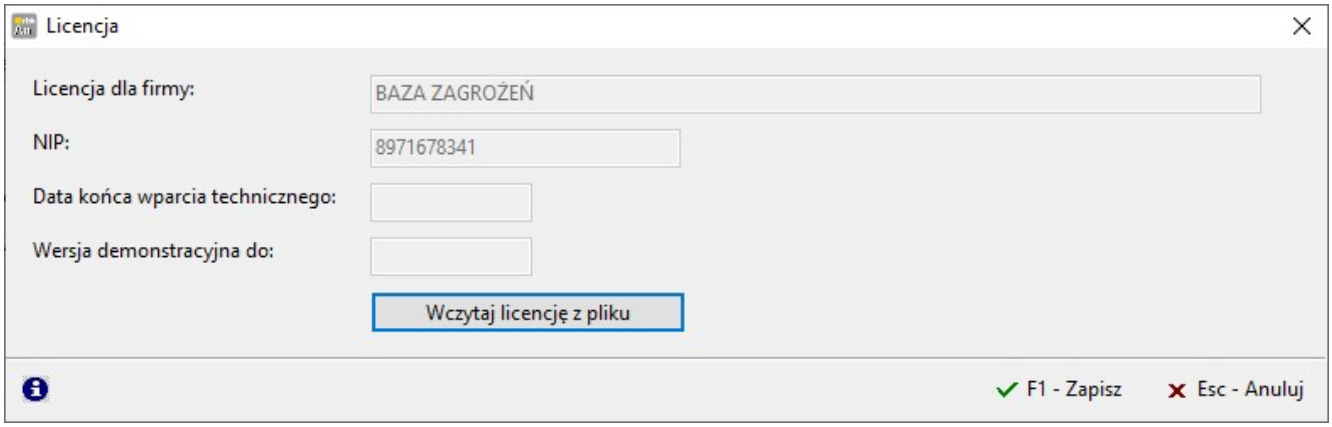
1. Zmiana parametrów możliwa jest wyłącznie na uprawnieniach **administratora.**
2. Konfigurację programu zmieniamy w zakładce **parametry.**



3. Aktualizacja licencji.
   Nową licencję dodajemy na zakładce ‘Parametry systemu’.

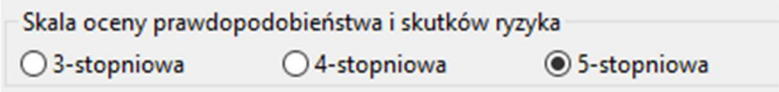


Przechodzimy do zakładki ‘Parametry programu i baz danych’, wybieramy przycisk ‘Licencja programu’ następnie ‘Wczytaj licencję z pliku’ wskazujemy przesłany plik licencji.
Plik powinien mieć rozszerzenie.lic. Zawartość pliku opisuje typ licencji, dane kontrahenta oraz przypisane kontrahentowi nr seryjny wykorzystywany do pobierania ryzyk online.



4. **Ustawienie skali,** w zakresie którym przeprowadzana będzie analiza.

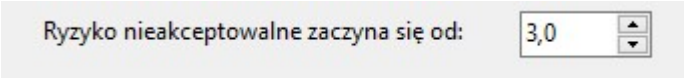
   Program umożliwia wybór skali trzystopniowej, czterostopniowej i pięciostopniowej. Zmianę skali realizuje się przestawiając znacznik.



Zmianę skali można dokonać w dowolnym momencie pracy z programem. Zalecamy na etapie testowania wybrać odpowiednią skalę. Zmiana skali w trakcie użytkowania programu wymusza zmianę metodyki, zmianę opisów dla wartości atrybutów oraz przestawienie progu ryzyka akceptowalnego i progu przeglądu. Zaleca się wykonywanie tej czynności wraz z serwisem programu. Wszystkie wykonane wcześniej ryzyka utracą status wykonanej oceny. **Wcześniej zrób kopie bazy!**

5. **Określenie progu,** w którym ryzyko będzie zmieniało ustawienia na nieakceptowalne.

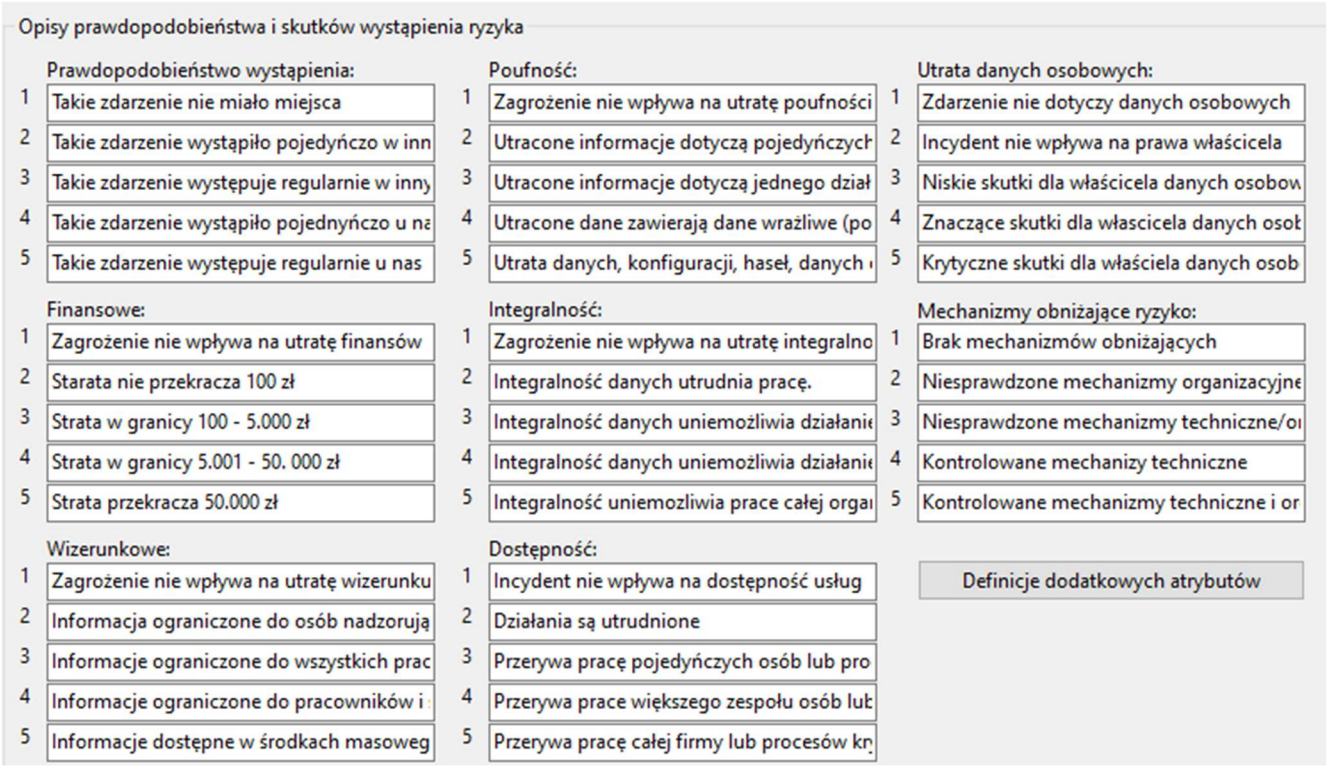
   Aplikacja standardowo ustawiona jest na wartość 3,0.
   Możliwa jest zmiana w zakresie od 1 do 5. Wartości poniżej 3,0 spowodują większą ilość ryzyk nieakceptowalnych i w związku z tym będą wymagane wysokiej jakości mechanizmy zabezpieczające. Skala powyżej 3,0 powoduje, że analiza staje się mniej wymagająca.



6. Określenie wymaganych opisów.

   Przed przystąpieniem do oceny, program do poprawnej pracy wymaga opisów:
   - prawdopodobieństwa,
   - skutków finansowych,
   - skutków wizerunkowych,
   - skutków utraty poufności,
   - skutków utraty integralności
   - skutków utraty dostępności,
   - skutków utraty danych osobowych,
   - mechanizmów obniżających ryzyko.

Opisy zostały przygotowane zgodnie z metodyką IMNS AnRisk Matrix.



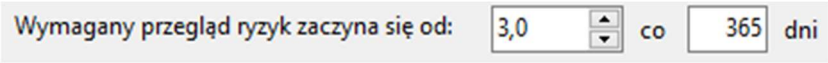
W przypadku, gdy będziecie Państwo modyfikować opisy należy **uzupełnić metodykę zarządzania ryzykiem**.

7. Określenie dodatkowych opisów.

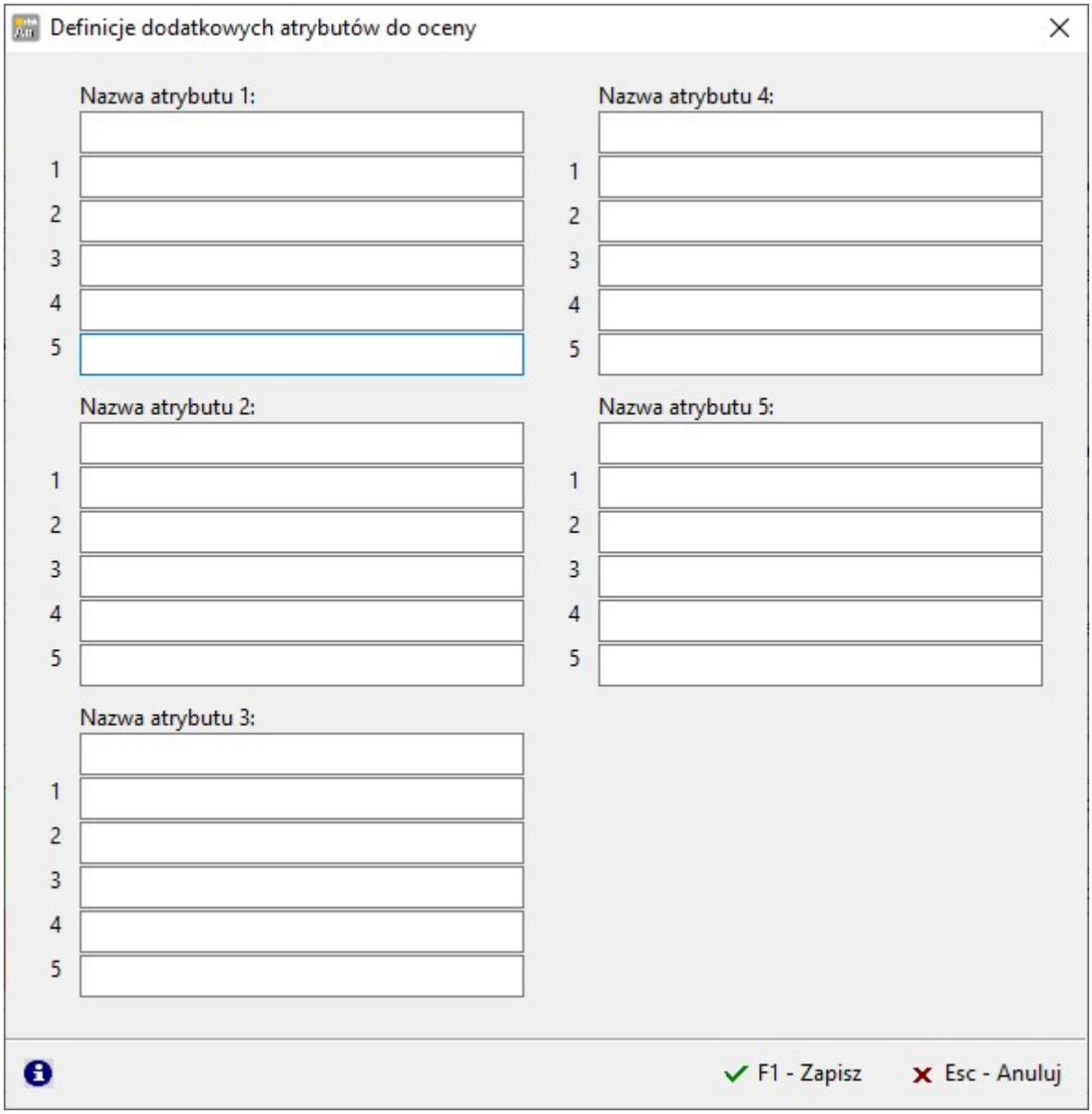
   Program umożliwia określenie własnych pięciu atrybutów do dodatkowej oceny. Wstępnie zdefiniowane zostały trzy:

   - Możliwość detekcji – pozwalająca ocenić możliwość wykrycia ryzyka.
   - Wpływ zdarzenia na inny proces.
   - Zakres danych osobowych utracanych na skutek zdarzenia.

8. Określenie parametrów przeglądu.



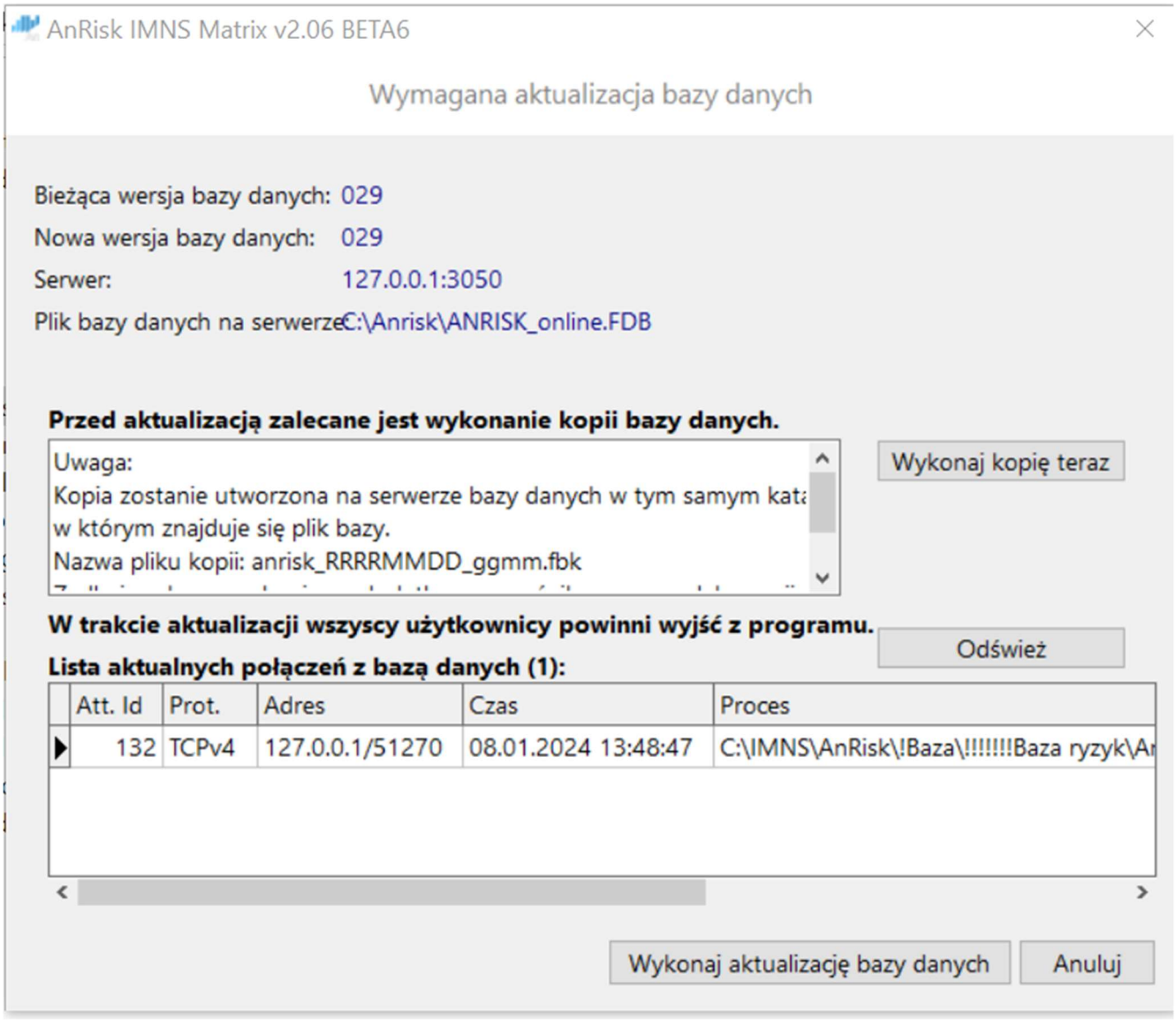
   Program umożliwia określenie progu, od którego ryzyka zostaną wskazane do oceny.
   Zalecany poziom to 3. W przypadku gdy ryzyko wstępne osiągnie taki poziom program zweryfikuje, które ryzyka nie były oceniane w ciągu ostatnich 365 dni. Częstotliwość przeglądu można indywidualnie definiować, wartość domyślna to 365.



Zmiana konfiguracji w programie jest możliwa w dowolnym momencie. Zmiana w czasie pracy skutkuje obowiązkiem ponownej kontroli przeprowadzonych ryzyk. Zaleca się niezmienianie parametrów, po wykonaniu dużej ilości analiz.
Przed zmianą skali należy zrobić kopię zapasową programu.

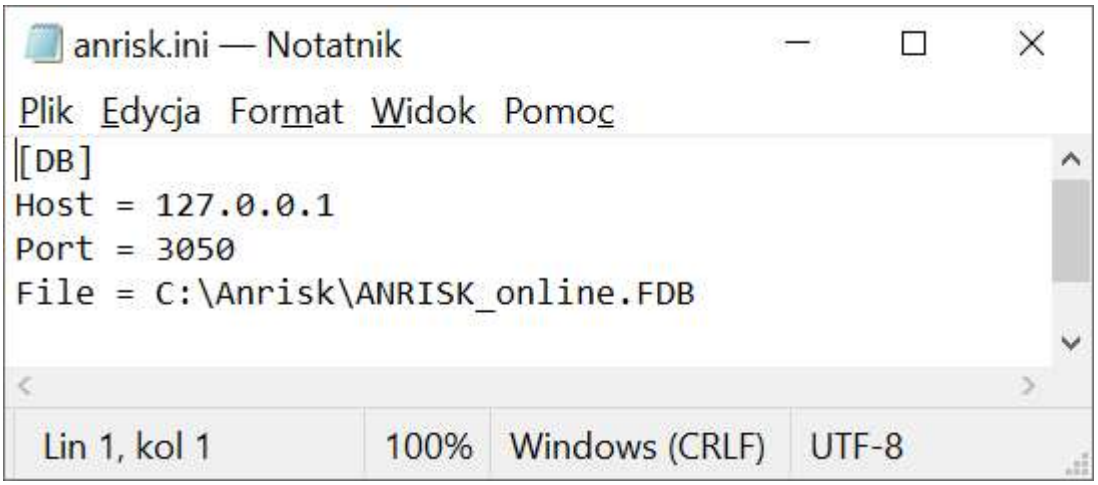
5) Kopie zapasowe.

Kopię zapasową można wykonać „ręcznie” klikając na przycisk Wykonaj kopię teraz oraz podczas aktualizacji programu.

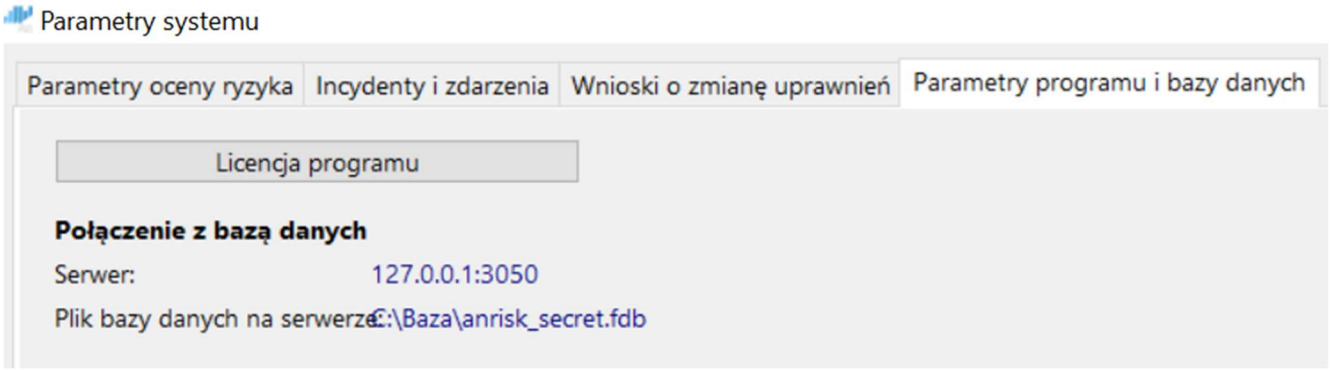


Zaleca się, aby objąć kopią cykliczną plik bazy danych wskazany w konfiguracji programu. Aby zweryfikować, gdzie znajduje się plik należy:

a) Otworzyć plik anrisk.ini znajdujący się w katalogu aplikacji, linia zaczynająca się od File oznacza lokalizację pliku z bazą danych.



b) Miejsce przechowywania pliku bazy można zweryfikować również w aplikacji na zakładce Parametry, zakładka Parametry programu i bazy danych.



6) Powiadomienia e-mailem.

1. Aplikacja AnRisk umożliwia informowanie użytkowników o zdarzeniach, które występują w programie np.:

- ilość nowych ryzyk, w których przekroczony został termin wdrożenia planu postępowania,

- ilość nowych ryzyk, w których należy przeprowadzić przegląd,

- ilość nowych ocen zdefiniowanych w KRI,

- ilość nowych zgłoszeń i incydentów o statusie „zarejestrowane”,

- ilość wniosków dotyczących uprawnień.

2. Konfiguracja programu AnRisk.

a) Aktualizacja programu AnRisk do najnowszej wersji.

b) Zakładamy osobne konto pocztowe, które będzie wykorzystywane do wysyłania powiadomień.

c) Na zakładce Parametry wybieramy Powiadomienia e-mail i ustawiamy konfigurację serwera pocztowego.

d) Definiujemy jakie informacje będą wysyłane.

e) Konfigurujemy częstotliwość analizy zdarzeń i wysyłania wiadomości. Wartość domyślna 15 minut.

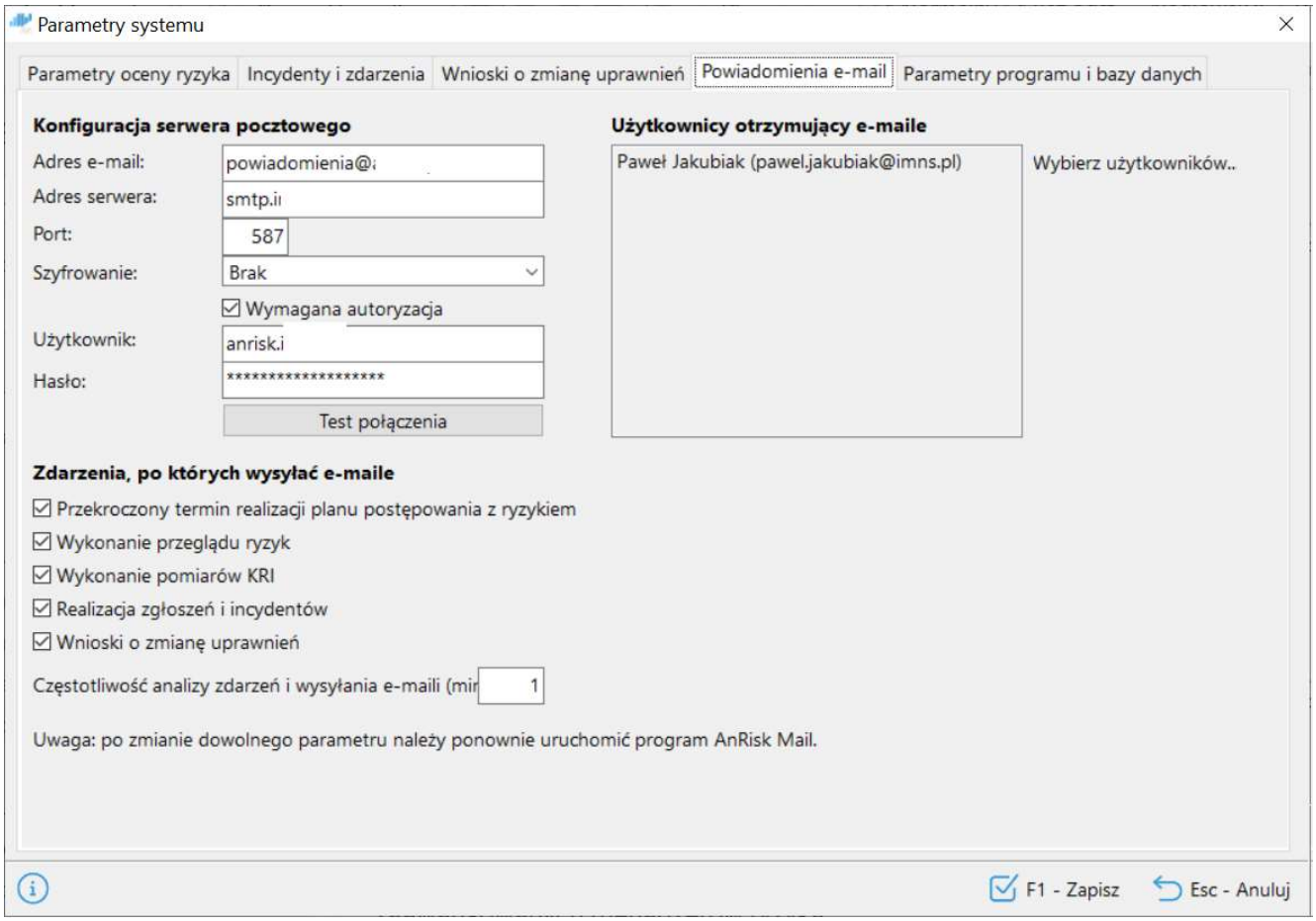
f) Wybieramy użytkowników, którzy będą otrzymywać wiadomości.

Użytkownik, który ma otrzymywać wiadomości musi mieć uprawnienia pozwalające na odczyt (procesów, komponentów, ryzyk, ocen ryzyka, zdarzeń i incydentów, wnioski o zmianę uprawnień).

3. Konfiguracja AnRisk Mail.

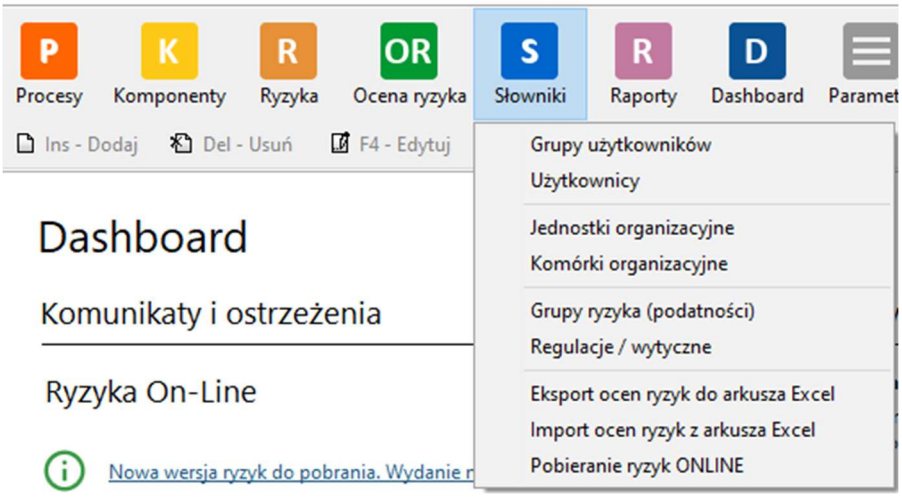
a) Katalog zaleca się umieścić w lokalizacji, gdzie znajduje się serwer bazy (nie jest to wymaganie, program z bazą kontaktuje się w ten sam sposób co klient za pomocą protokołu TCI IP).

b) Do katalogu AnRiskMail należy skopiować plik anrisk.ini, który znajduje się w katalogu głównym aplikacji.
c) Pliki z katalogu DLL należy skopiować do głównego katalogu aplikacji oraz do katalogu z którego uruchamiany jest AnRisk Mail.
d) Uruchamiamy aplikację, która będzie w cyklu odpytywała bazę AnRiska i wysyłała komunikaty.
e) Na serwerze powinien być dostęp do portu SMTP waszego serwera pocztowego.
f) Standardowo wykorzystywane są porty Explicit 587 i Implicit 465 wybierając odpowiedni port ustal to z administratorem serwera pocztowego.

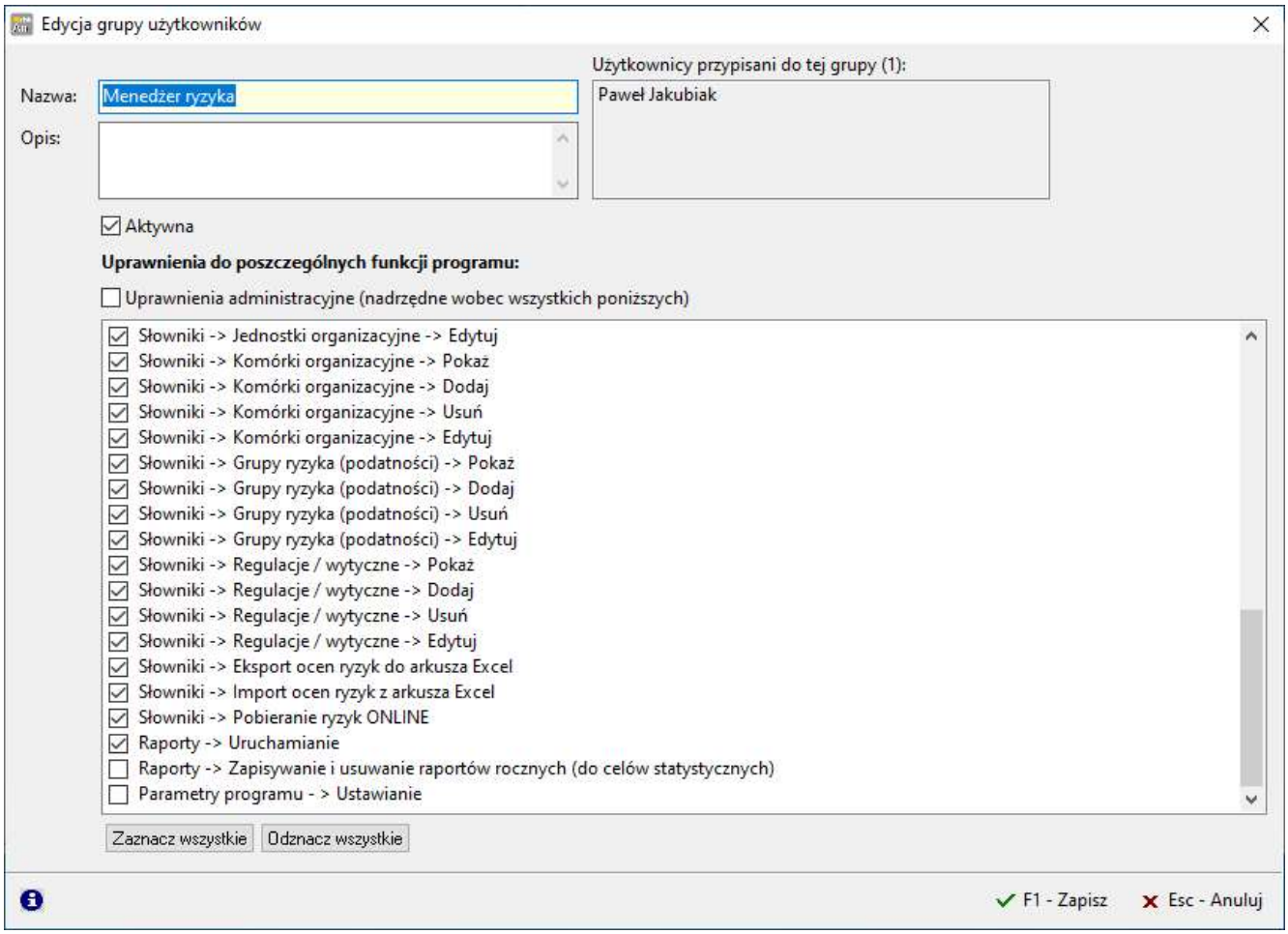


Słowniki.

Uprawnienia do opcji słowniki powinny być dostępne wyłącznie dla administratorów oraz zaawansowanych menadżerów ryzyka.



Grupy użytkowników.



Program umożliwia użytkowanie dowolnej ilości grup użytkowników. Standardowo utworzone są trzy grupy:

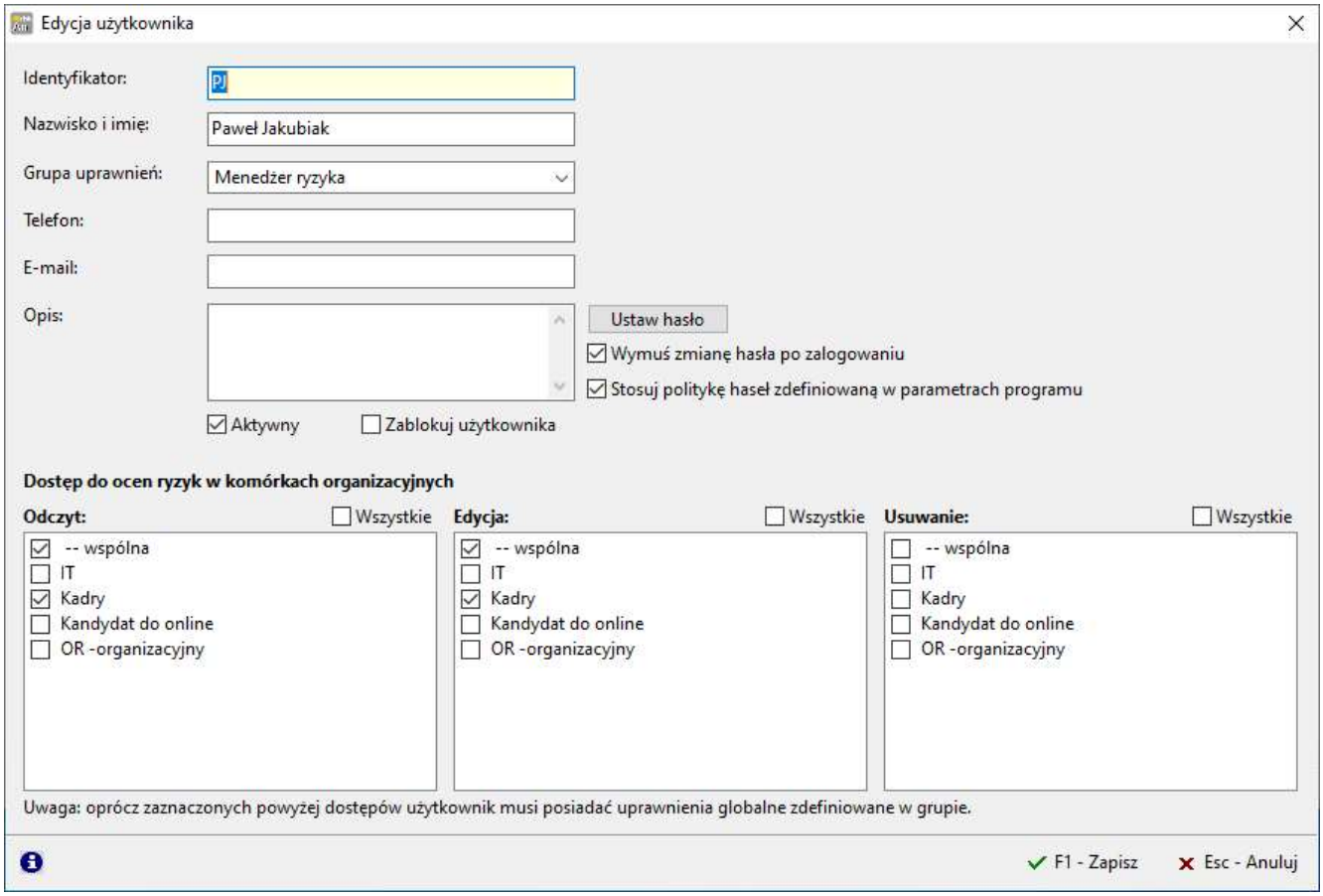
- Administrator – posiadający pełne uprawnienia do aplikacji.
- Menadżer ryzyka – posiadający ograniczenia związane z zarządzaniem uprawnieniami, tworzeniem raportów rocznych oraz zmianami parametrów.
- Tylko do odczytu – użytkownik z przypisana tą grupą nie ma możliwości modyfikowania programu.

Zakres uprawnień umożliwia określenie czterech uprawnień do funkcji programu w zakresie:

- Pokaż – umożliwienie wyświetlania zawartości.
- Dodaj – dodawania nowych rekordów.
- Usuń – kasowania istniejących rekordów.
- Edytuj – edycji rekordów.

Zakładka ta pozwala na identyfikację wszystkich przypisanych osób do danej grupy

Użytkownicy.



Funkcja ta pozwala na:

- Zakładanie nowych użytkowników.
- Przypisywanie do ocen ryzyk w komórkach organizacyjnych (trzy poziomy Odczyt, Edycja, Usuwanie).
- Przypisywanie grupy uprawnień.
- Określanie danych kontaktowych.
- Zarządzania hasłami.

Jednostki organizacyjne.

Jeżeli jest taka potrzeba można wykorzystać funkcję ‘Jednostki organizacyjne’ do odwzorowania schematu organizacyjnego.

Jednostki organizacyjne

Nazwa	Opis	Ile komórek	Aktywna
-- brak		2	Tak
DI	Departament Informatyczny	1	Tak
OK	Obsługa klienta	0	Tak
WF	Wydział finansowy	1	Tak
WO	Wydział organizacyjny	3	Tak

Funkcję można wykorzystać na dowolnym etapie użytkowania programu.

Komórki organizacyjne.

Podstawowym mechanizmem kontroli dostępu użytkownika do ocenianych ryzyk jest przypisanie do komórki organizacyjnej. W programie należy odwzorować komórki organizacyjne i pojedyncze stanowiska, zgodnie ze strukturą organizacyjną.

Grupy ryzyka (podatności).

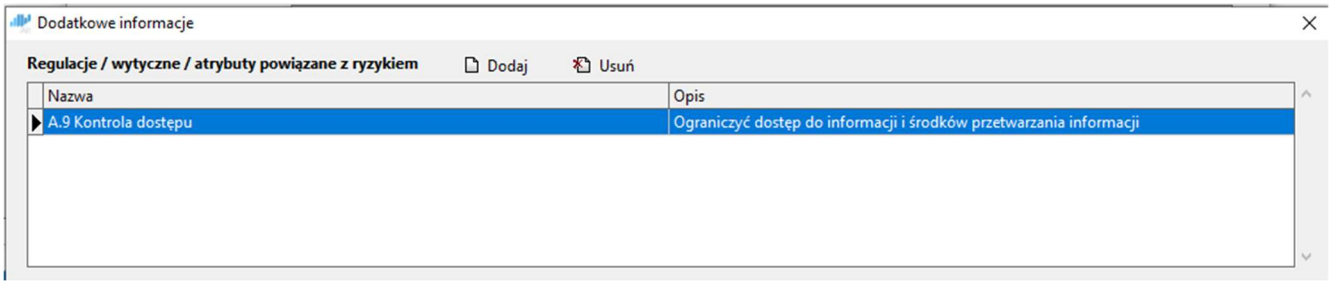
W celu ułatwienia filtracji aplikacja umożliwia przypisanie ryzyka do własnych grup ryzyka (podatności). Możliwe jest stworzenie dowolnej ilości grup ryzyka. Ryzyko może być przypisane tylko do jednej grupy.

Grupy ryzyka (podatności)

Nazwa	Opis	Aktywna
Błędy administratora	Błędy, zaniedbania, brak wiedzy administratora	Tak
Błędy pracownika	Błędy, zaniedbania, brak wiedzy.	Tak
Błędy pracownika firmy zewnętrznej	Błędy, zaniedbania, brak wiedzy pracownika firmy zewnę	Tak
Błędy programisty	Błędy generowane na etapie tworzenia aplikacji	Tak
Chmura	Grupa ryzyk związana z przetwarzaniem danych w chmu	Tak
Ciągłość działania	Zapewnienie ciągłości działania	Tak
Cyberprzestępczość	Działania przestępcze	Tak

Regulacje / wytyczne / atrybuty.

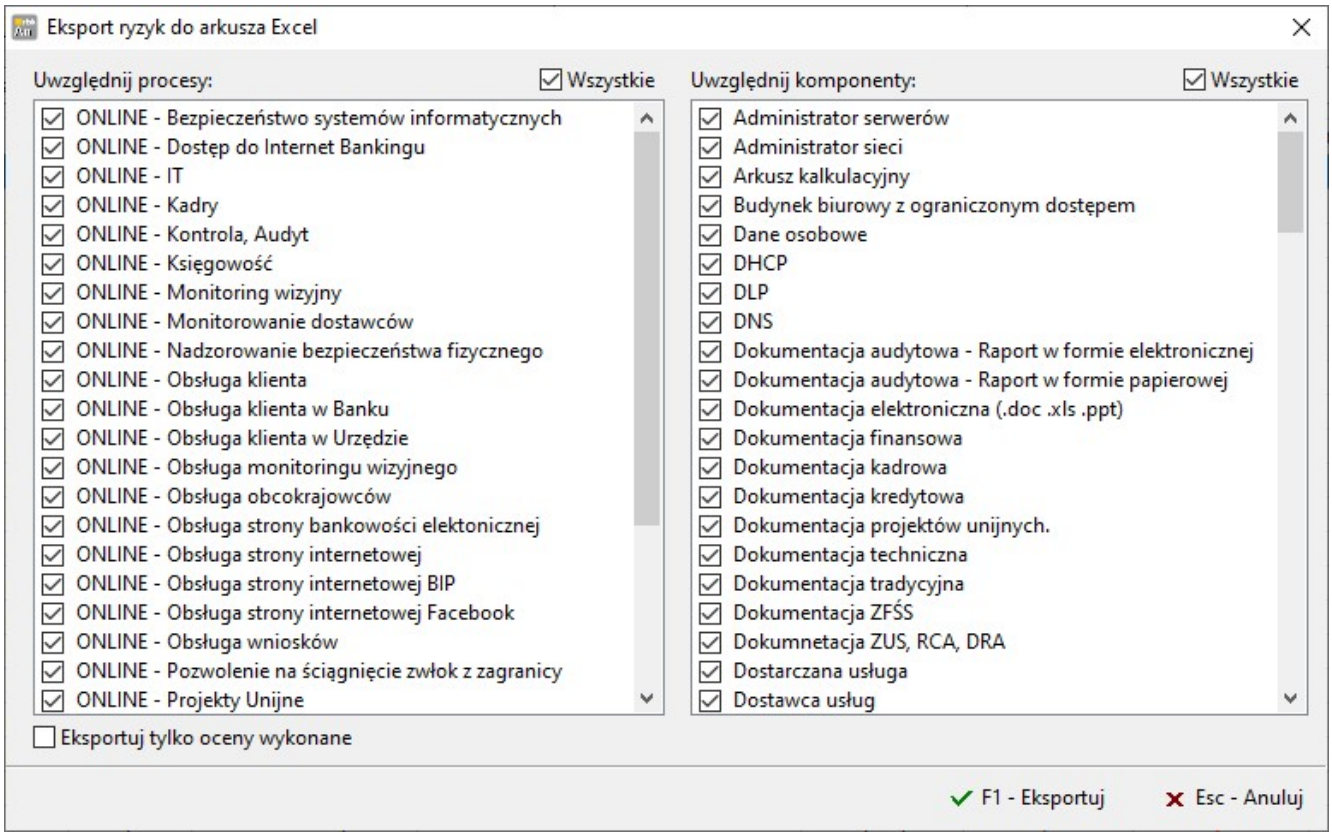
1. Funkcja ta może zostać wykorzystana w programie do grupowania ryzyk, na podstawie wprowadzonych atrybutów, np., chcemy połączyć w grupę wszystkie ryzyka, które zostały zidentyfikowane po audycie lub połączyć ryzyka z przepisem prawa, wytyczną, dokumentacją wewnętrzną lub frameworkiem bezpieczeństwa.
2. Na tej zakładce możemy dodawać, kasować, edytować lub eksportować do Excela atrybuty.
3. Aby dodać nowy atrybut należy wprowadzić nazwę oraz opis.
4. Wprowadzone atrybuty można wiązać z ryzykiem podczas oceny ryzyka wchodząc w **„Dodatkowe informacje”.**



5. Ryzyka powiązane atrybutami można raportować wykorzystując szablon raportu **„Raport ryzyk wg regulacji / wytycznych / atrybutów”.**

Eksport ocen ryzyk do arkusza Excel.

1. W zakładce **Słowniki** znajdują się przyciski importu i eksportu do Excela.



2. Istnieje możliwość wyboru procesów i komponentów, które mają zostać wyeksportowane.

Import ocen ryzyk z arkusza Excel.

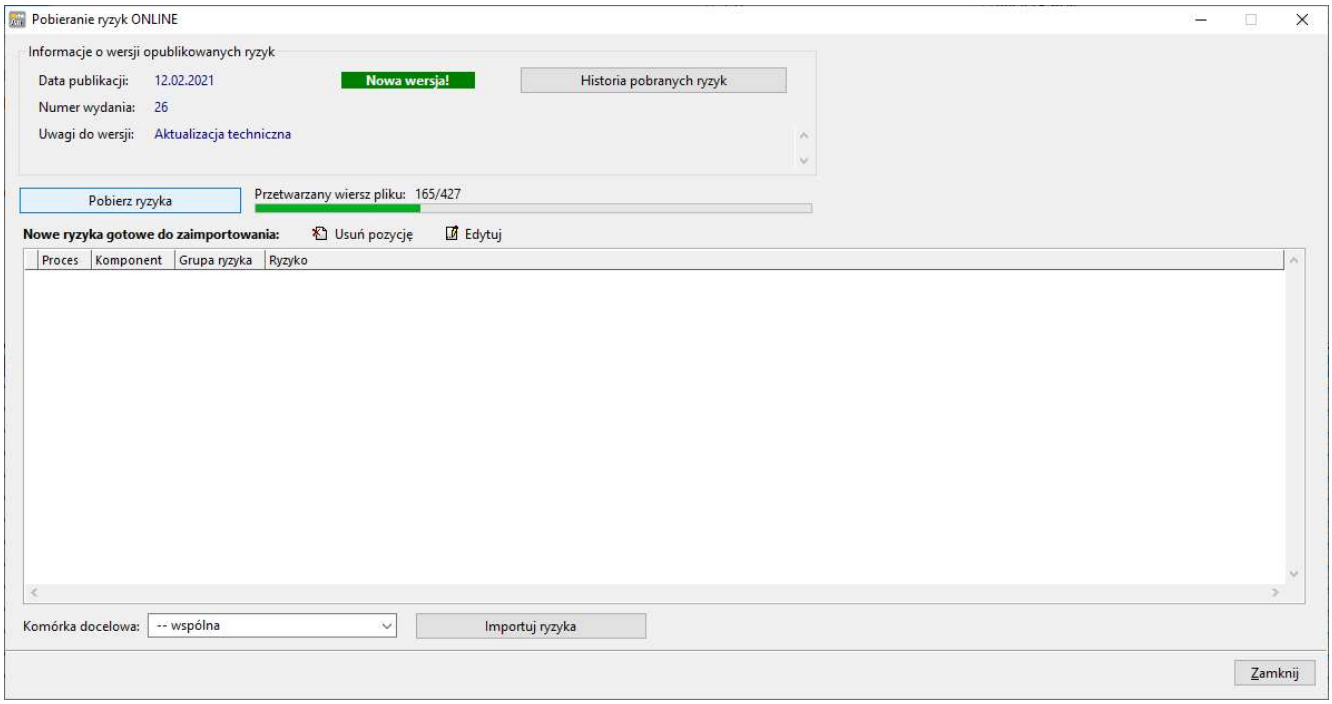
1. Importując ryzyka należy zapewnić odpowiedni format danych.
2. Import zaczyna się od wiersza trzeciego, kolejne kolumny oznaczają:

Kolumna	Typ danych	Pole wymagane
A	**Nazwa procesu**	T
B	Opis procesu	N
C	Kategorie danych	N
D	Miejsce, w którym odbywa się proces	N
E	Uwagi do procesu	N
F	Dane osobowe wrażliwe w procesie	N
G	**Nazwa komponentu**	T
H	Opis komponentu	N
I	**Grupa ryzyka**	T

J	Opis grupy ryzyka	N
K	**Nazwa ryzyka**	T
L	Opis ryzyka	N
M	**Wartość szacowania prawdopodobieństwa**	T
N	Wartość szacowania strat finansowych	T
O	Wartość szacowania strat wizerunkowych	T
P	Wartość szacowania strat związanych z poufnością	T
Q	Wartość szacowania strat związanych z integralnością	T
R	Wartość szacowania strat związanych z dostępnością	T
S	Wartość szacowania strat związaną z utratą danych osobowych	T
T	Mechanizmy obniżające ryzyko	T
U	Opis skutków utraty danych	T
V	Opis mechanizmów obniżających ryzyko	T

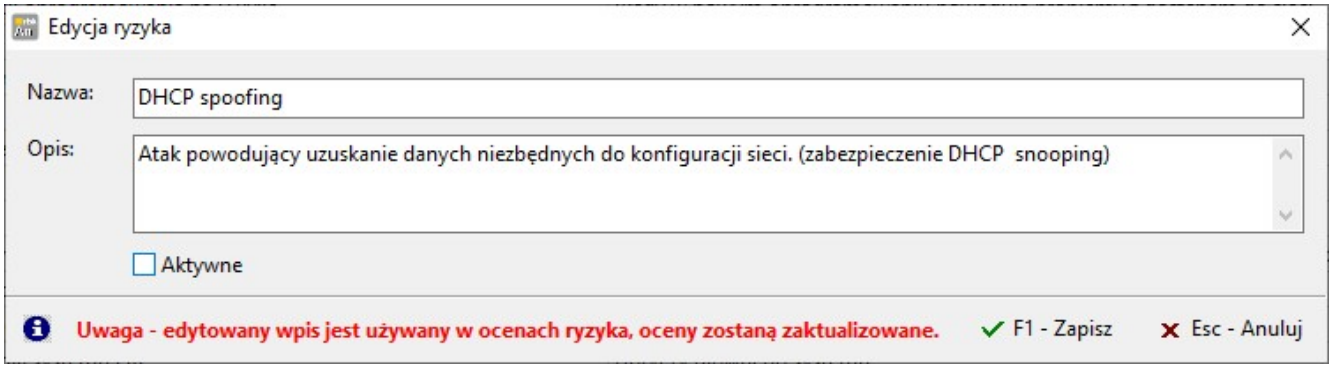
Pobieranie ryzyk ONLINE.

1. Import ryzyk uruchamia się wchodząc w **Słowniki** i wybierając **Pobieranie ryzyk online.**



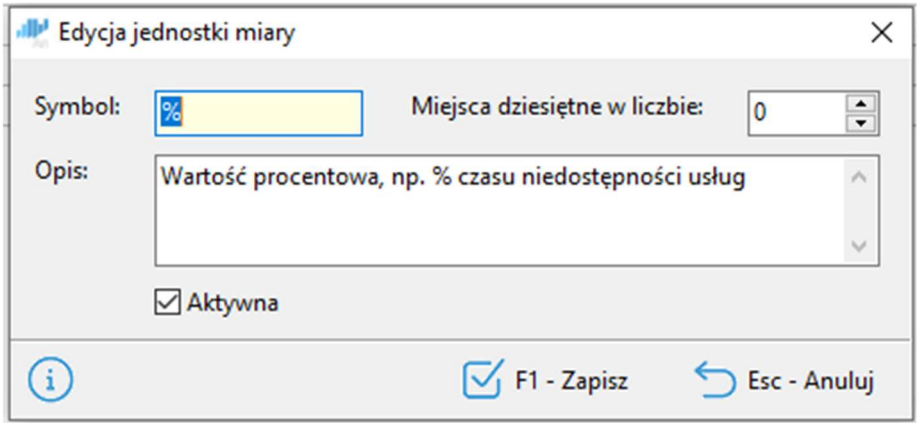
2. Pobierając ryzyka zaleca się zaimportowanie wszystkich ryzyk do programu.
3. Zaimportowane ryzyka posiadają wstępną ocenę prawdopodobieństwa oraz propozycję oceny atrybutów.
4. Przy pierwszym pobieraniu ryzyk należy przypisać je do Komórki '—wspólna' aby móc przypisać procesy odpowiednim komórkom. Kolejne ryzyka można przypisywać indywidualnym komórkom.
5. Istnieje możliwość usunięcia proponowanego ryzyka lub jego edycji.

W przypadku nieadekwatnych ryzyk np. brak takiego komponentu, zaleca się zaimportować wszystkie ryzyka, następnie w zakładce Ryzyka wyszukać niepotrzebne ryzyko i odznaczyć **Aktywne.**



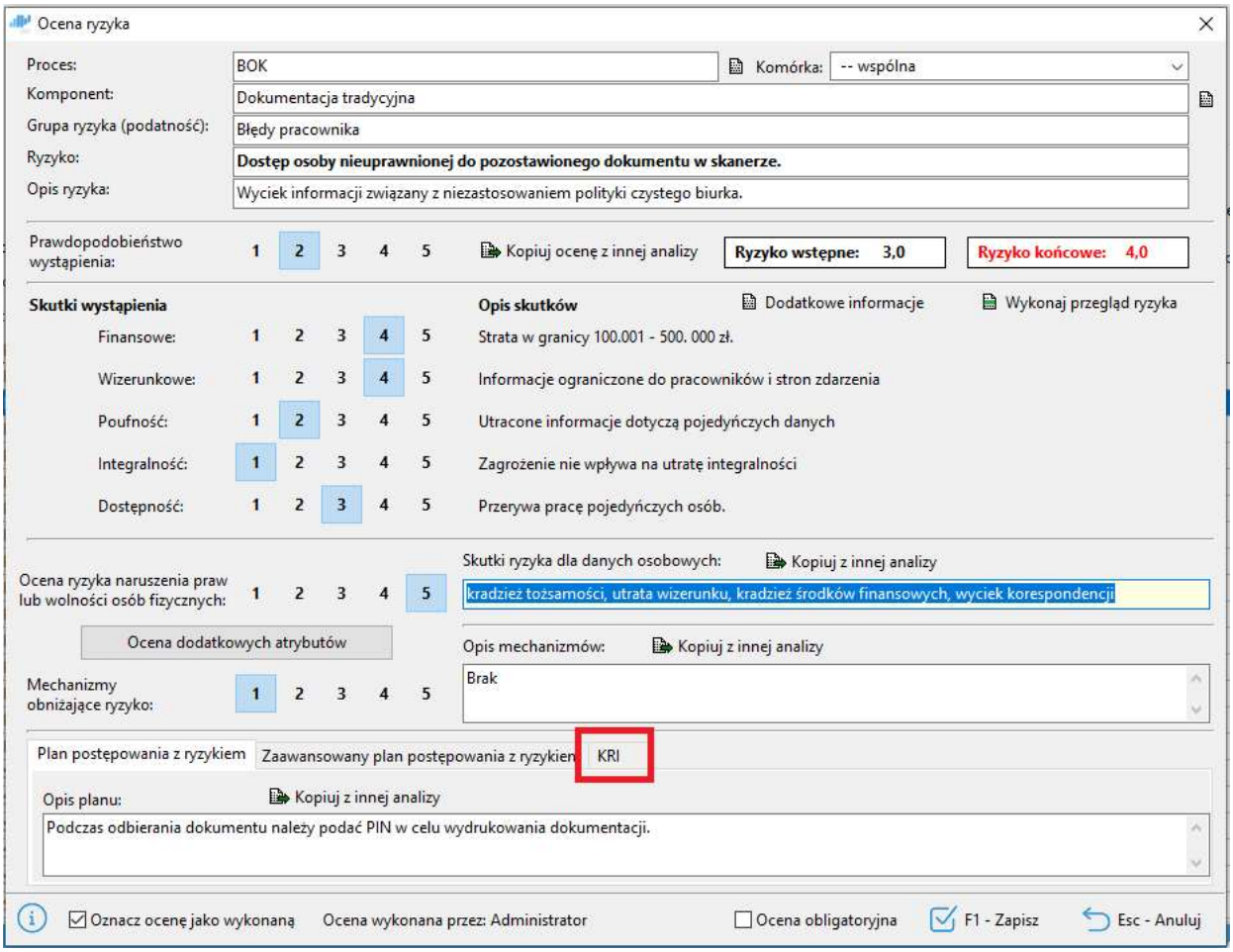
KRI – Jednostki miar Key Risc Inficators (kluczowe wskaźniki ryzyka).

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.

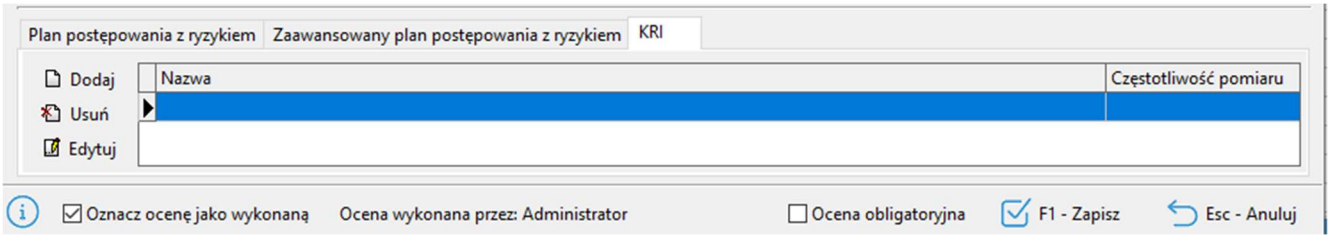


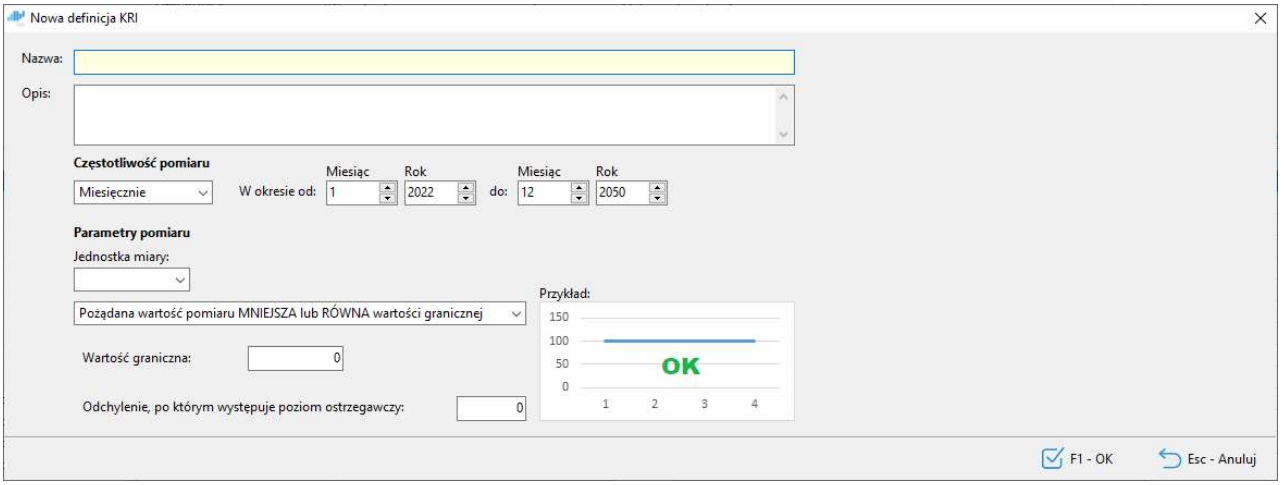
Dodanie KRI do ryzyka.

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



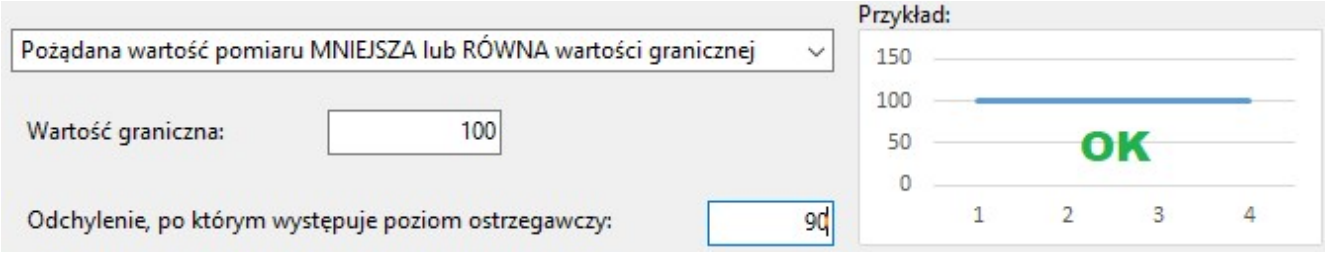
2. Zakładka KRI umożliwia dodawanie nowego mechanizmu pomiarowego, usuwanie oraz edycję KRI.



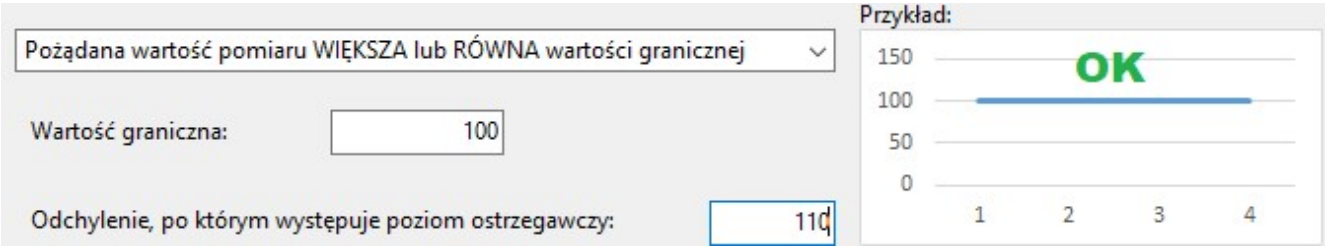


3. Dodając nowy mechanizm pomiarowy definiuje się:

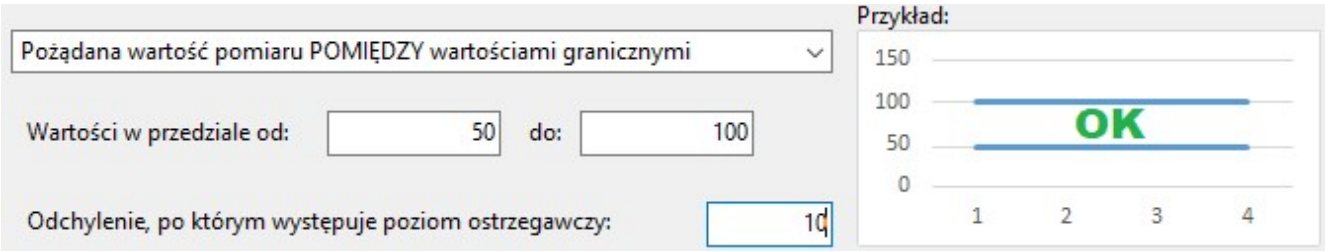
- Nazwę KRI.
- Opis.
- Częstotliwość pomiaru (roczna, półroczna, kwartalna, miesięczna).
- Jednostki miary (nowe jednostki definiuje się w menu Słowniki > KRI > Jednostki miar).
- Wybór mechanizmu pomiaru, pożądana wartość pomiaru **mniejsza lub równa** wartości granicznej.



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

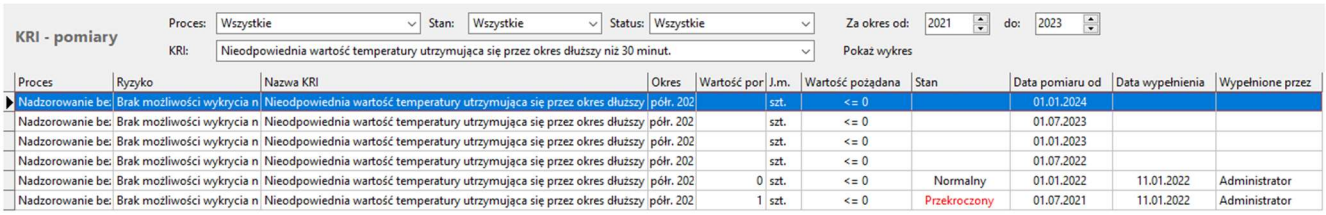


- Wybór mechanizmu pomiaru, pożądana wartość pomiaru **w przedziale od do.**



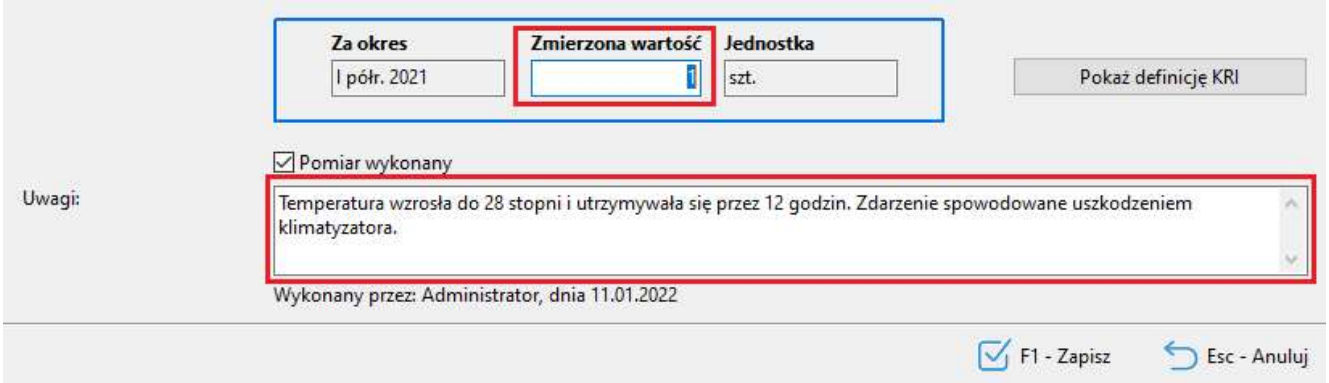
KRI – Pomiary.

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



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	półr. 202		szt.	<= 0		01.01.2024		
Nadzorowanie be:	Brak możliwości wykrycia n	Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy	półr. 202		szt.	<= 0		01.07.2023		
Nadzorowanie be:	Brak możliwości wykrycia n	Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy	półr. 202		szt.	<= 0		01.01.2023		
Nadzorowanie be:	Brak możliwości wykrycia n	Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy	półr. 202		szt.	<= 0		01.07.2022		
Nadzorowanie be:	Brak możliwości wykrycia n	Nieodpowiednia wartość temperatury utrzymująca się przez okres dłuższy	półr. 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	półr. 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.

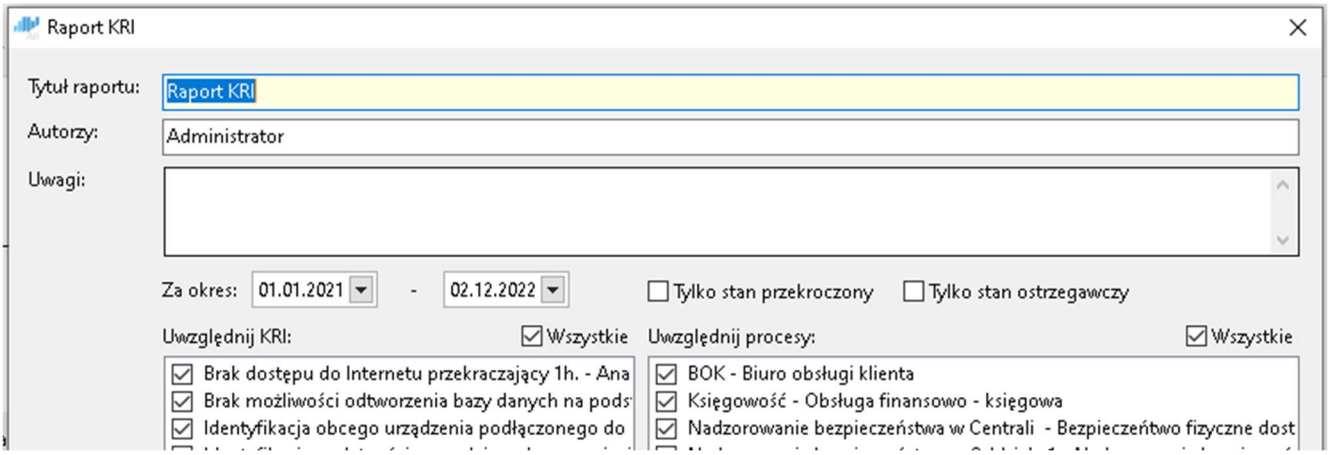


Raportowanie KRI.

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.

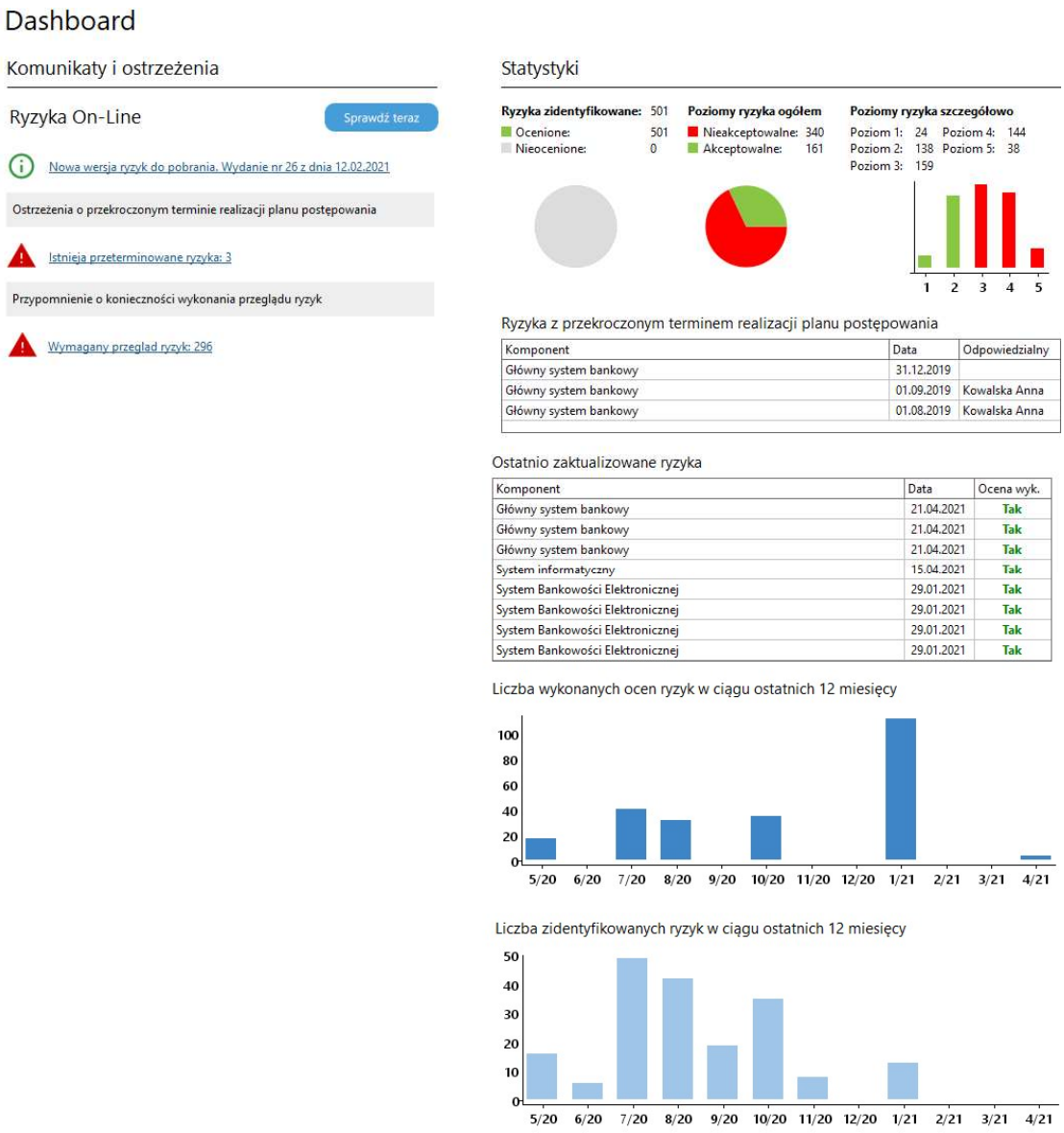


Menadżer ryzyka

Dashboard.

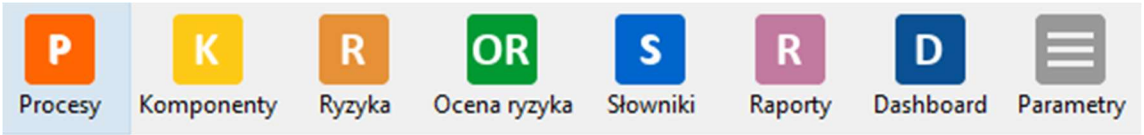
1. Informacje dostępne w Dashboard-ie aplikacji zawierają:
    - Informację o nowych ryzykach on-line.
    - Ostrzeżenia o przekroczonym terminie realizacji planu postepowania.
    - Informację o konieczności przeprowadzenia przeglądu ryzyk.
    - Statystyki ilości ryzyk ocenionych i nieocenionych.
    - 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 wciągu ostatnich 12 miesięcy.
- Ilość KRI wymagających uzupełnienia.



Dodanie procesu.

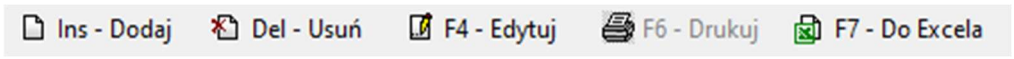
1. Definicja procesów realizowana jest w zakładce „Procesy”.



2. Identyfikacja procesów obejmuje:

- nazwę procesu,
- opis procesu,
- kategorię przetwarzanych danych,
- przypisanie komórki organizacyjnej zdefiniowanej w słowniku,
- miejsce przechowywania,
- informację o danych wrażliwych przetwarzanych w procesie,
- informację o komponentach wykorzystywanych w procesie.

3. Panel zakładki procesy.



Ins – Dodaj – umożliwia dodanie nowego procesu.

Del – Usuń – umożliwia skasowanie wybranego procesu.

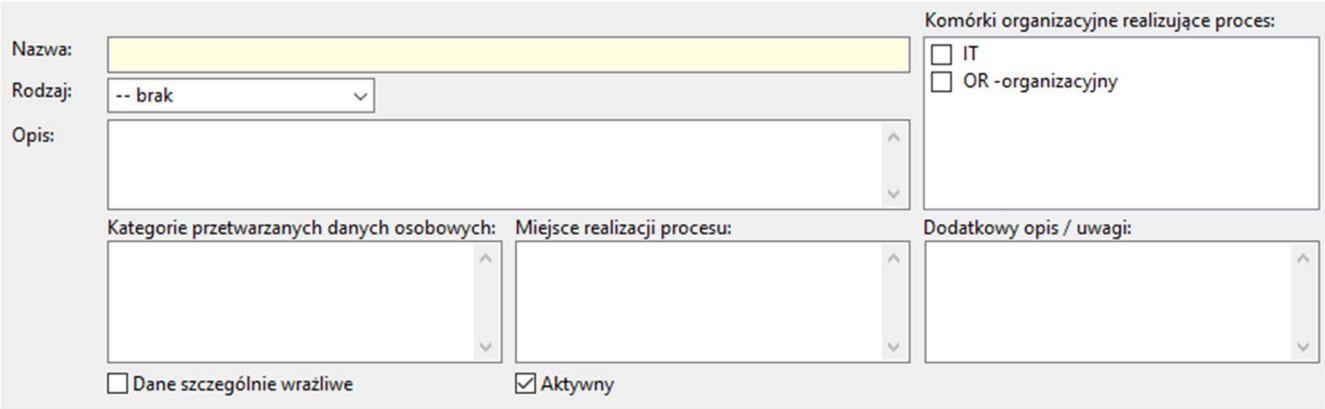
F4 – Edytuj – pozwala na wprowadzenie zmian w procesie.

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.



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

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.).

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

Dodatkowy opis / uwagi – pole umożliwia wprowadzenie dodatkowych opisów.

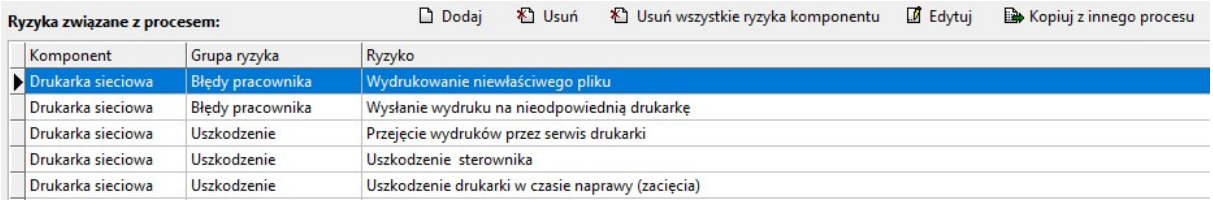
Dane szczególnie wrażliwe – należy zaznaczyć, jeżeli w ramach procesu przetwarzane są dane określone w art. 9 RODO.

Komórki organizacyjne realizujące proces – w przypadku, gdy proces realizowany jest w wielu komórkach organizacyjnych, należy powiązać dany proces z odpowiednimi komórkami.

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).

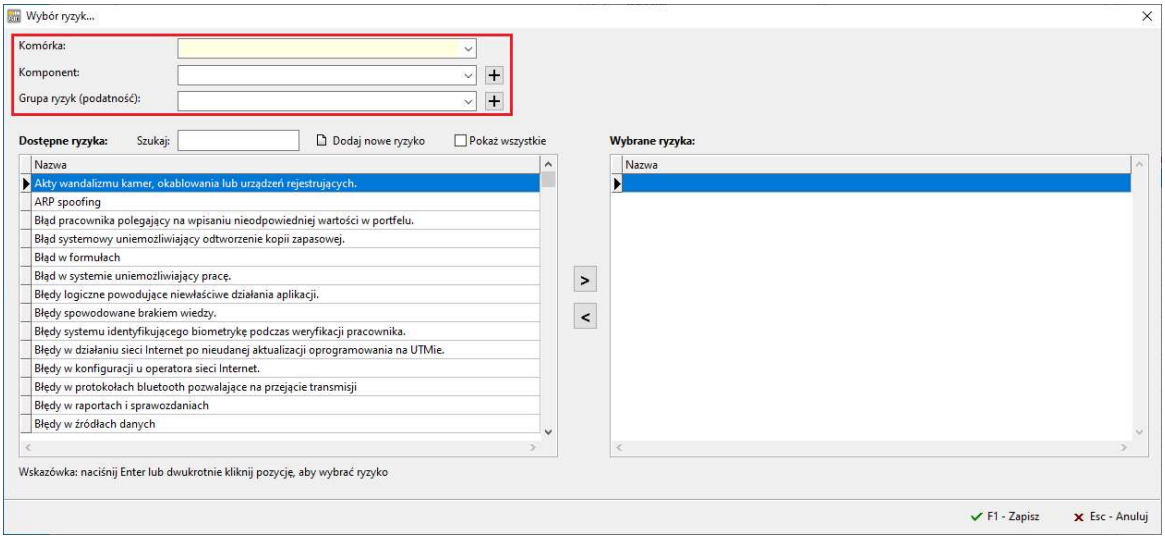
5. Lista ryzyk przypisanych do procesu.



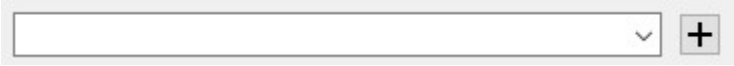
Zakładka Edycja **procesu** umożliwia przypisanie do procesu.

6. Dodanie nowego ryzyka.

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

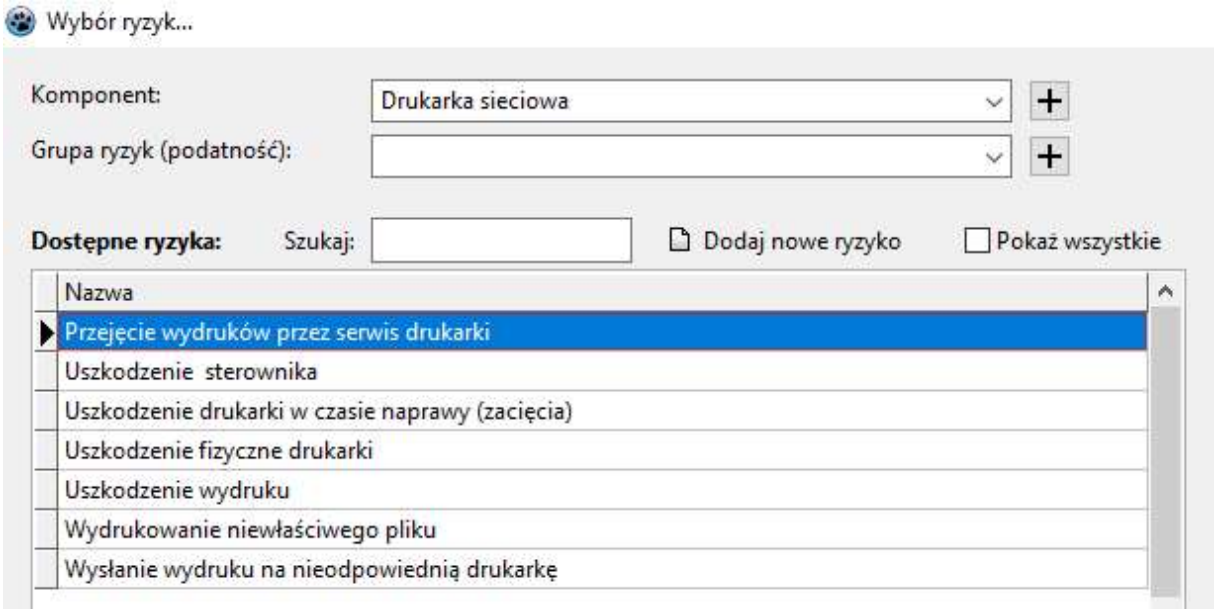


Wybranie istniejącego komponentu i grupy ryzyk umożliwia pole wyboru.

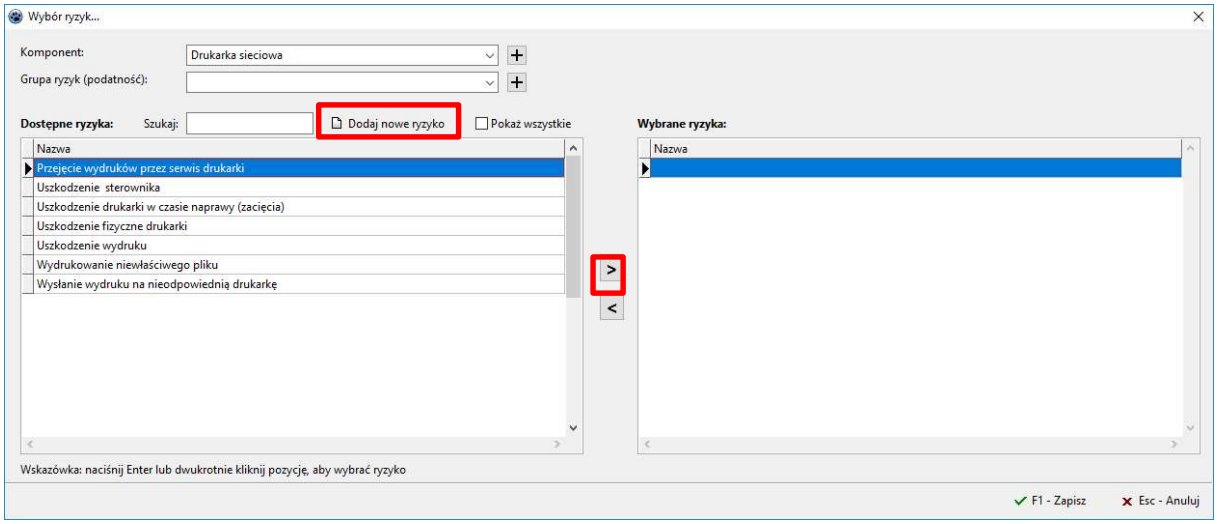


W przypadku dodana nowego komponentu lub grupy ryzyka należy kliknąć znak plusa.

7. Wybranie istniejącego komponentu wyświetla przypisane do niego ryzyka.

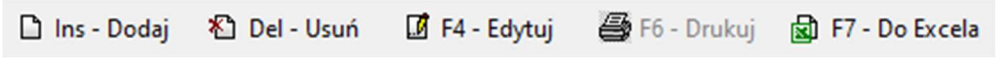


Można wybrać dostępne ryzyka klikając na znak > lub dodać nowe ryzyko.



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 komponencie.

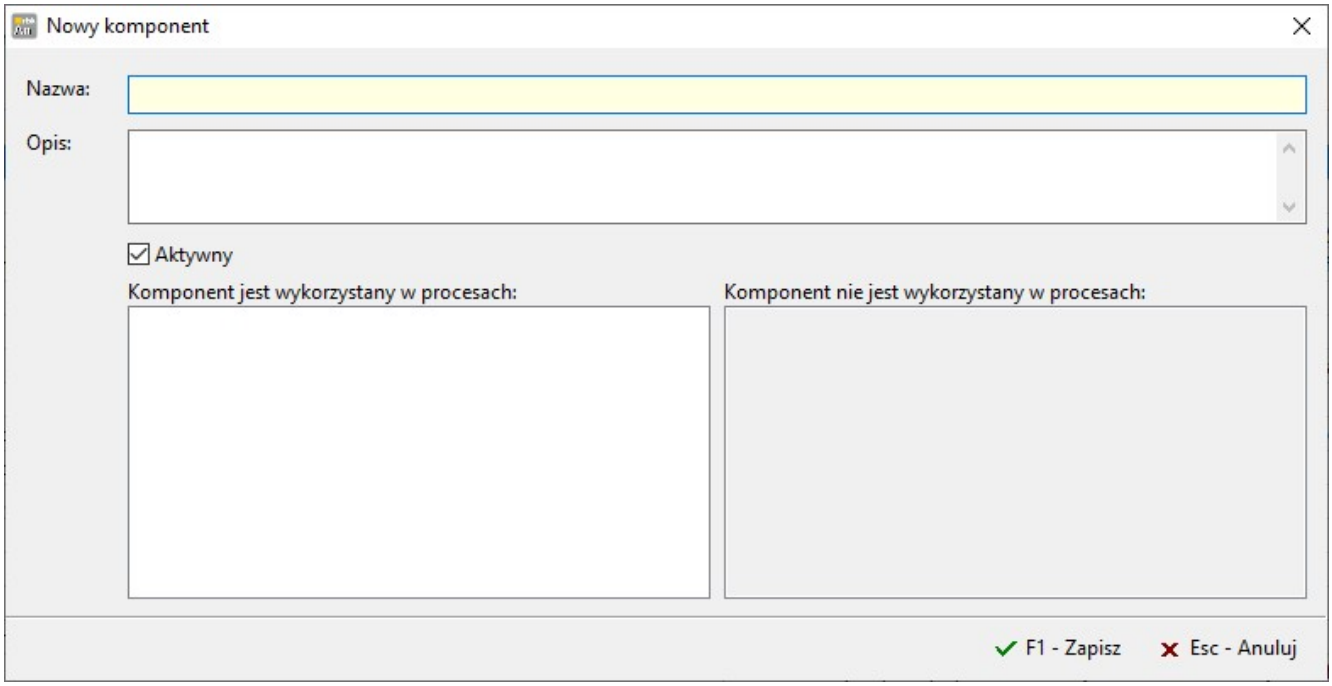
F6 – Drukuj – drukowanie nieaktywne na tym widoku

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

2. Widok komponentów zawiera kolumny:

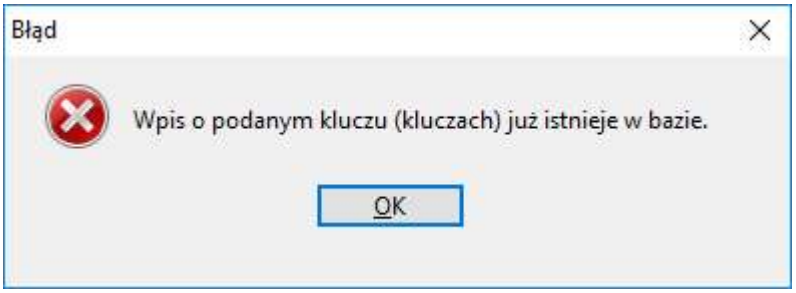
- Nazwa - nazwa komponentu.
- Opis – opis komponentu.
- Wykorzystano – informuje czy komponent jest powiązany z procesem.
- Aktywny - informacja czy komponent zostanie uwzględniony w raporcie.

3. **Dodanie** nowego komponentu.

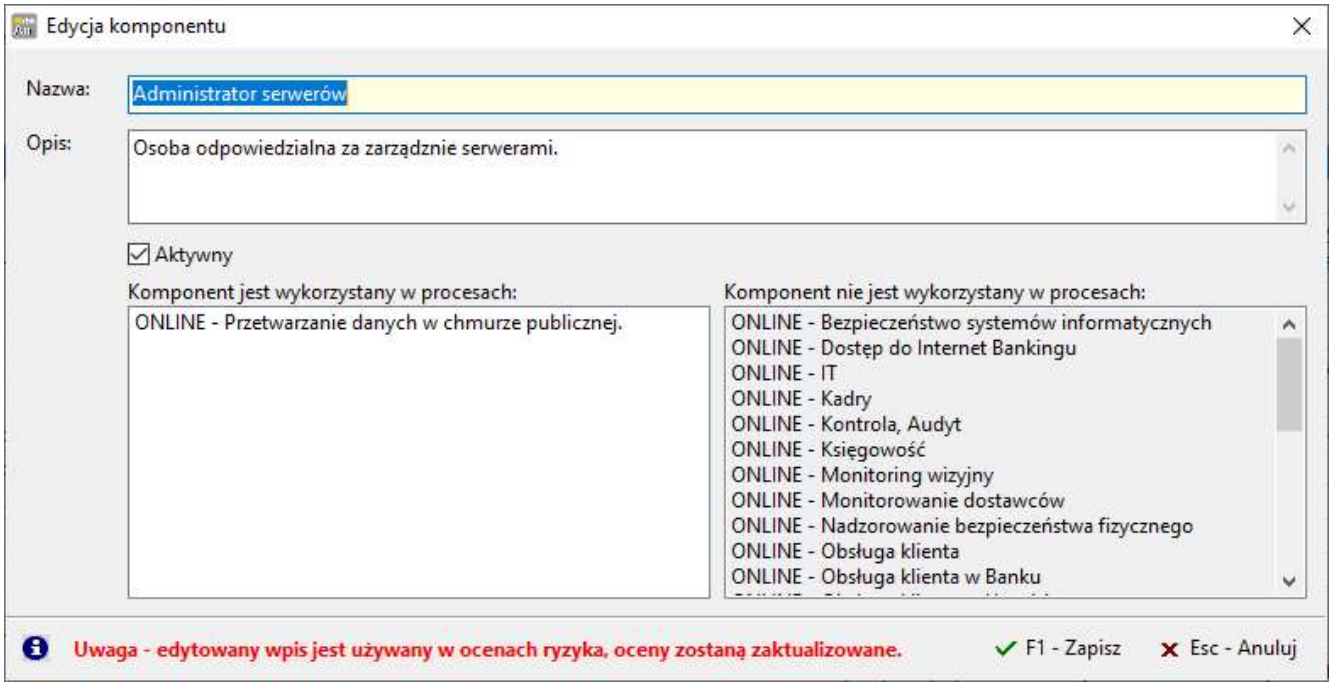


W celu dodania nowego komponentu wystarczy wypełnić pola tekstowe nazwa i opis.

Program nie umożliwia wprowadzenia dwóch komponentów o takiej samej nazwie.
Wyświetli komunikat.

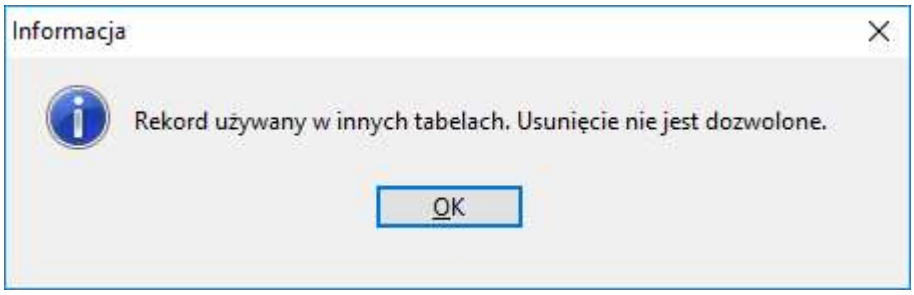


4. **Edycja komponentu** pozwana na kontrolę powiązań komponentów z procesami.



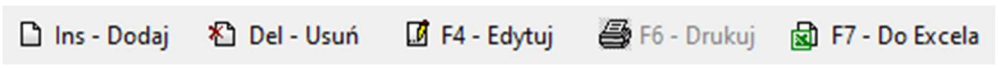
5. **Kasowanie komponentu** jest możliwe, jeżeli nie jest połączony z innymi procesami.

   Aplikacja poinformuje o niedozwolonej funkcji.



Edycja ryzyka.

1. **Panel** zakładki komponenty.



   Ins – Dodaj – umożliwia dodanie nowego ryzyka.

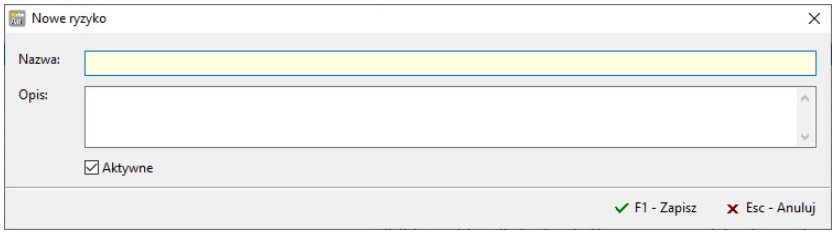
   Del – Usuń – umożliwia skasowanie wybranego ryzyka.

   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.

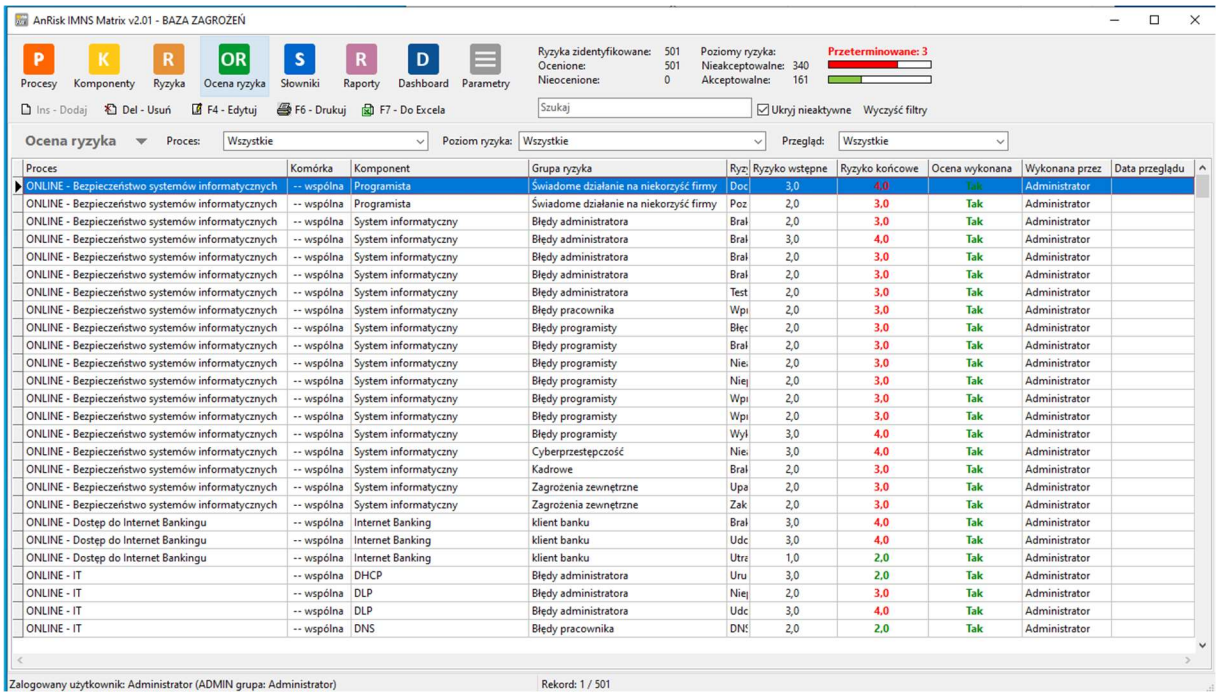
2. Widok ryzyk zawiera kolumny:
   - Nazwa - nazwa ryzyka.
   - Opis – opis ryzyka.
   - Aktywny - informacja czy ryzyko zostanie uwzględnione w raporcie.
3. Dodanie **nowego ryzyka.**



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’.



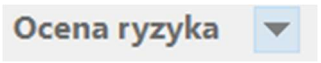
2. Filtrowanie podstawowe.

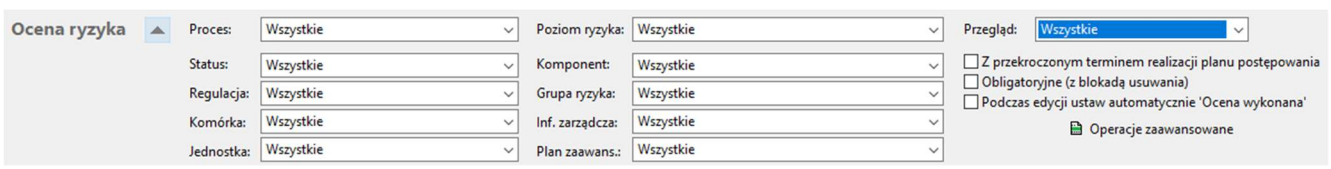
Umożliwia wyświetlenie wszystkich ryzyk z:

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

3. Filtrowanie rozszerzone.

Filtr rozszerzony uruchamia się za pomocą przycisku.

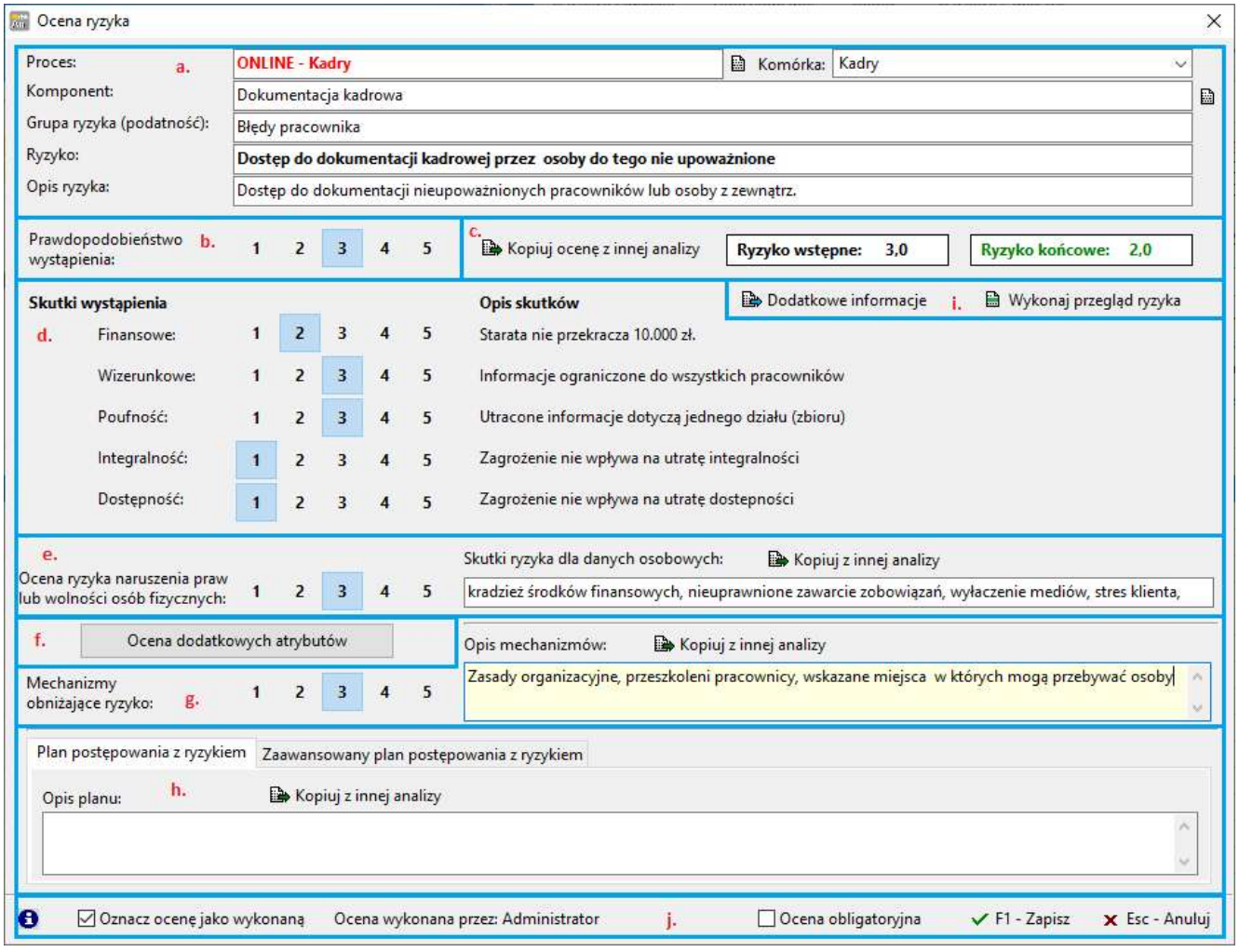




Aplikacja umożliwia filtrowanie w zakresie selekcji:

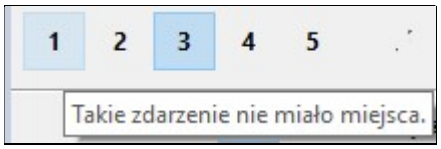
- Procesów – umożliwia wybranie ryzyk należących do jednego procesu.
- Statusu – umożliwia wybranie tylko tych ryzyk, których analiza została wykonana bądź niewykonana lub umożliwia wybór wszystkich ryzyk.
- Regulacji – umożliwia wybranie ryzyk przypisanych do regulacji.
- Komórki – umożliwia wybranie ryzyka przypisanego do komórki.
- Jednostki – jednostki organizacyjnej wprowadzonej do aplikacji.
- 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.
- Przeglądu – umożliwia wyświetlenie ryzyk wymagających przeglądu.
- Z przekroczonym terminem realizacji planu postępowania.
- Obligatoryjne – z blokadą usuwania.

Ocena ryzyka.

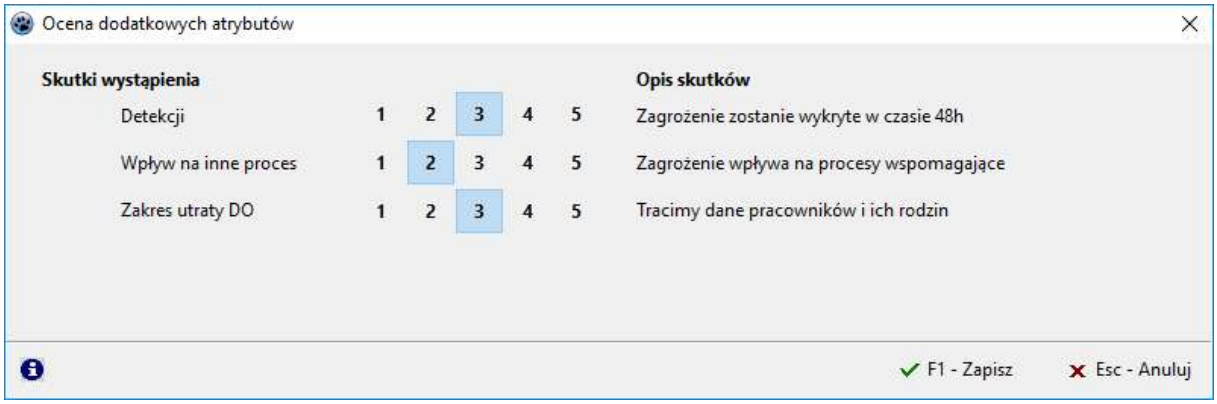


1. **W sekcji a** wyświetlane są informacje na temat ocenianego procesu oraz możliwość przypisania ryzyka innej komórce.
2. **W sekcji b** oceniane jest prawdopodobieństwo wystąpienia ocenianego ryzyka, zgodnie z przyjętą metodyką.

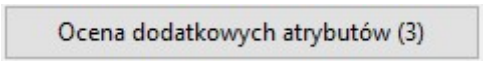
Wskazując kursorem na wartości liczbowe program podpowiada definicję danej wartości.



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**.



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



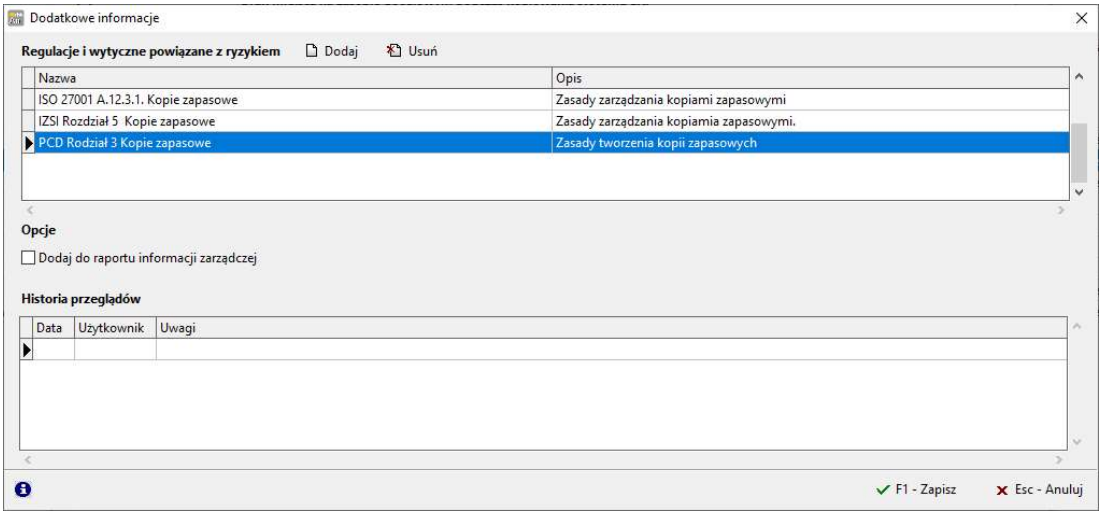
7. **Sekcja g** służy do określenia mechanizmów, które wpływają na obniżenie ryzyka.

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

8. **Sekcja h** służy do przygotowania planu postepowania z ryzykiem. W pierwszej zakładce wprowadza się opis.
Zakładka **zaawansowany plan postepowania z ryzykiem** służy do określenia szczegółów planu.

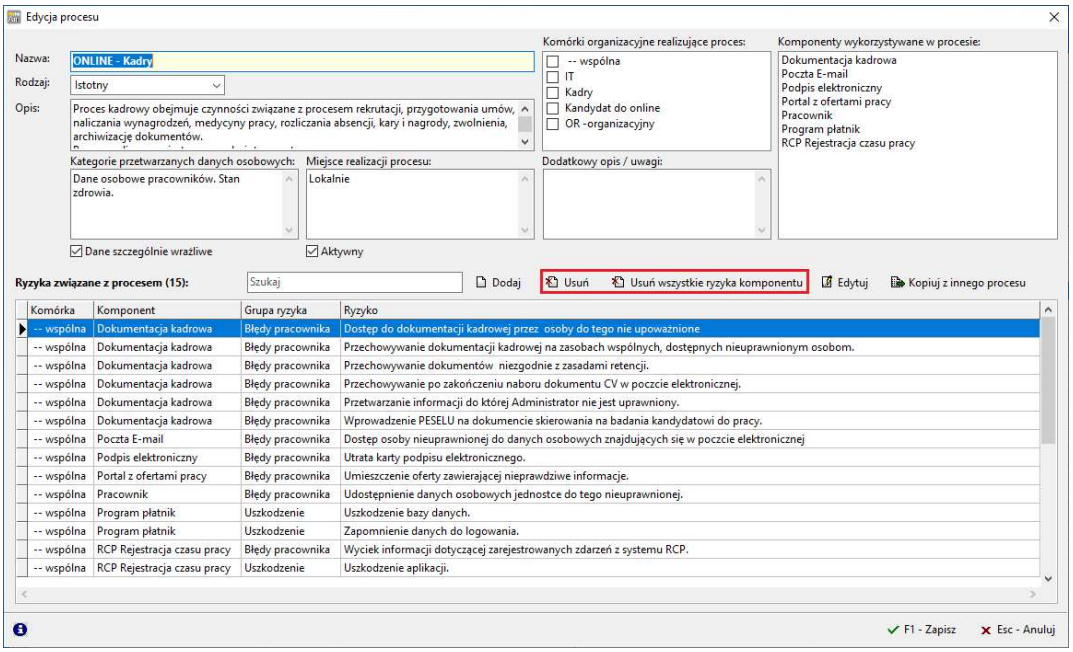
Plan postępowania należy wypełnić za każdym razem, gdy ryzyko osiągnie poziom nieakceptowalny.

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.



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

Kasowanie ryzyk w procesie.



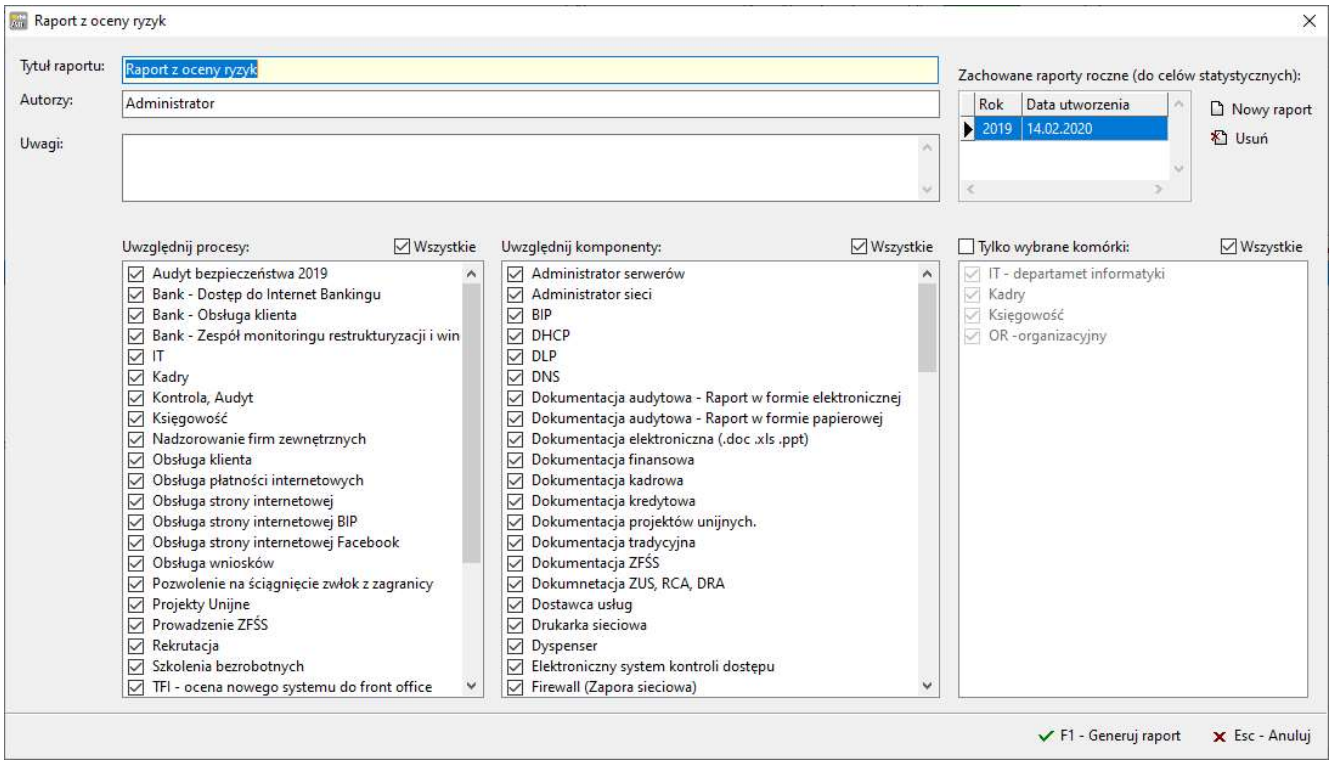
1. Przycisk ‘Usuń’ – usuwa podświetlone ryzyko.
2. Usuwanie wszystkich ryzyk z danego komponentu - w tym celu należy **‘zaznaczyć komponent’**, którego ryzyka mają zostać usunięte i kliknąć **‘Usuń wszystkie ryzyka z komponentu’.** W tym przypadku usuniętych zostanie 6 ryzyk dotyczących dokumentacji kadrowej.

Raportowanie.

1. Obecnie aplikacja umożliwia przygotowanie pełnego raportu z ryzyk, ryzyk dotyczących informacji zarządczej oraz raportu dotyczącego bezpieczeństwa danych osobowych.

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

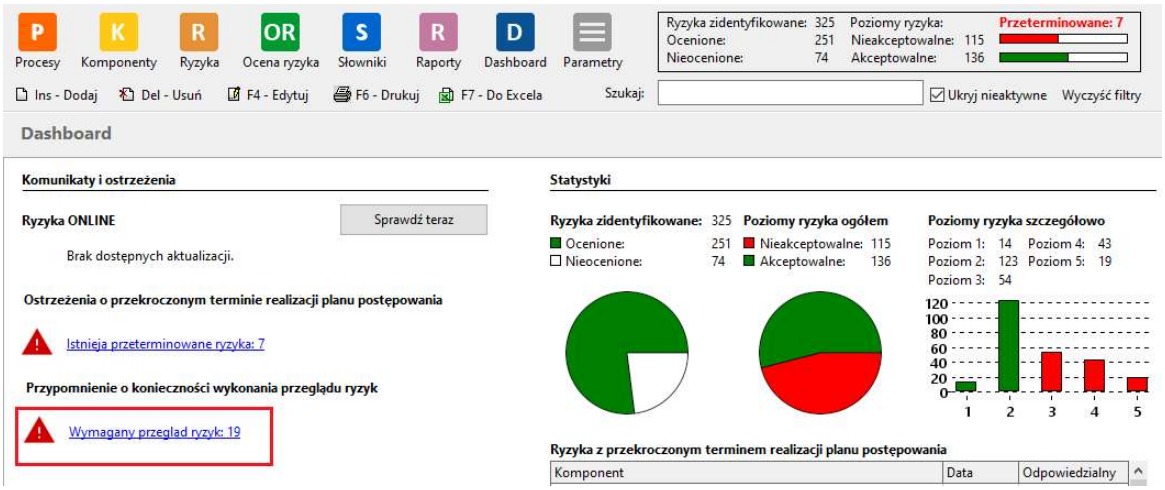
2. Generując raport istnieje możliwość określenia:
   - tytułu raportu,
   - informacji o autorach raportu,
   - uwag,
   - procesów i komponentów, które mają znaleźć się w raporcie.



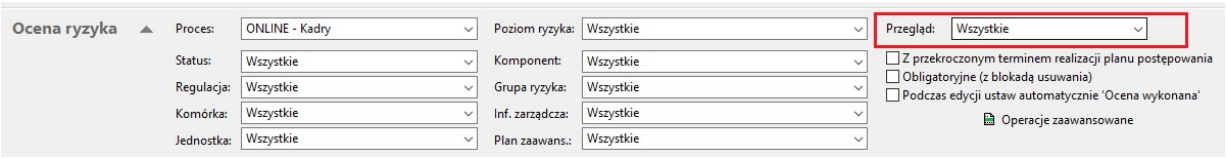
3. Funkcja Zachowane raporty roczne (do celów statystycznych) – generuje się po przekazaniu raportu do najwyższego kierownictwa. Raport uwzględniający zmiany pomiędzy raportami zostanie wprowadzony w kolejnych wersjach.

Przegląd ryzyka.

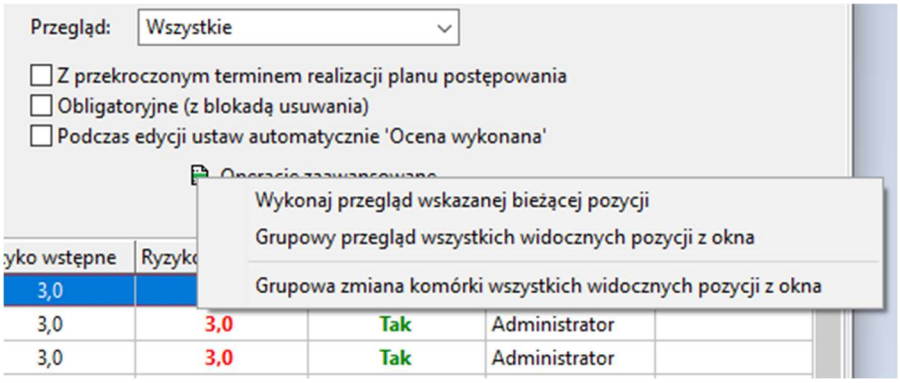
1. Ustawienie parametrów przeglądu opisane zostało w punkcie **Konfiguracja programu.**
2. Program informuje o ryzykach, które wymagają przeglądu. Informacja ta jest dostępna na Dashboardzie.



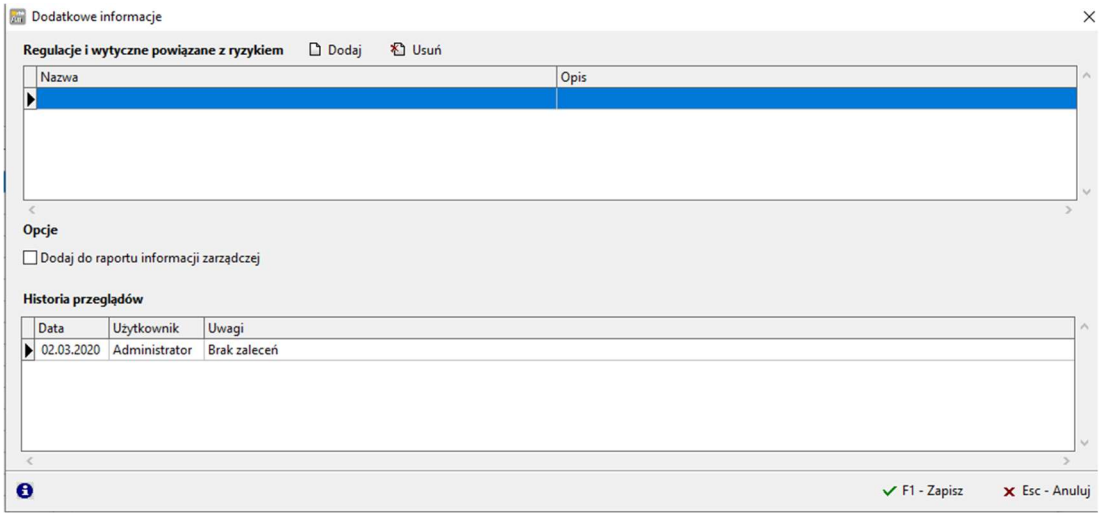
3. Za pomocą filtrów w **Ocenie ryzyka** możliwe jest wskazanie ryzyk wymagających przeglądu oraz ryzyk z wykonanym przeglądem.



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’.

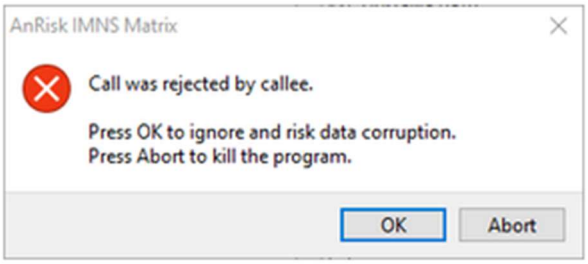


5. Informacja o przeglądzie jest widoczna na oknie informacji dodatkowych dla każdego ryzyka indywidualnie.



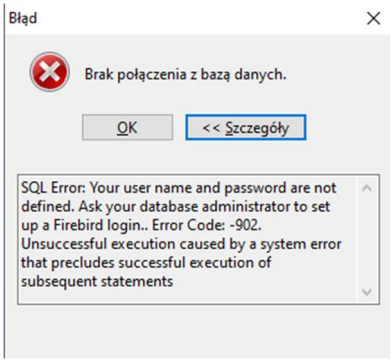
Rozwiązywanie błędów.

1. W programie Excel może pojawić się błąd otwarcia pliku Excel przez aplikacje AnRisk.



   Jest to najprawdopodobniej nową funkcją DDE (Dynamic Data Exchange).
   Należy dodać :
   \HKEY_CURRENT_USER\Software\Microsoft\Office*TwojaWersja*\Excel\Security
   Wartość DWORD - AllowDDE = 1

2. Wystąpienie błędu ‘Brak połączenia z bazą danych’ po instalacji aplikacji. Może być to spowodowane
   a) Ominięciem w procesie instalacji serwera skopiowania pliku ‘security3.fdb’ do katalogu, w którym jest serwer Firebirda.

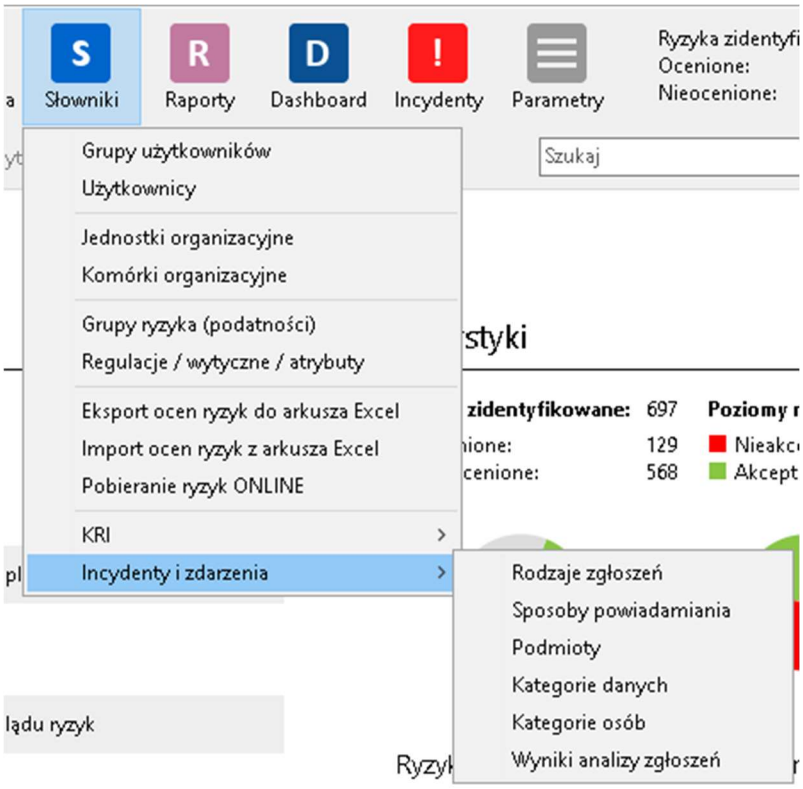


   b) Blokowanie przez zaporę portu 3050. Sprawdź czy ze stacji, na której ma być uruchomiony AnRisk jest dostępny zdalnie port 3050 (np. za pomocą aplikacji telnet).

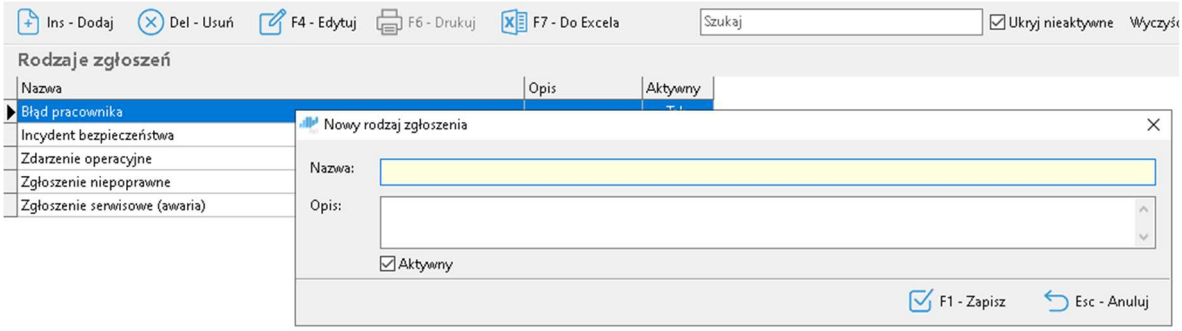
Zarządzanie incydentami

Konfiguracja.

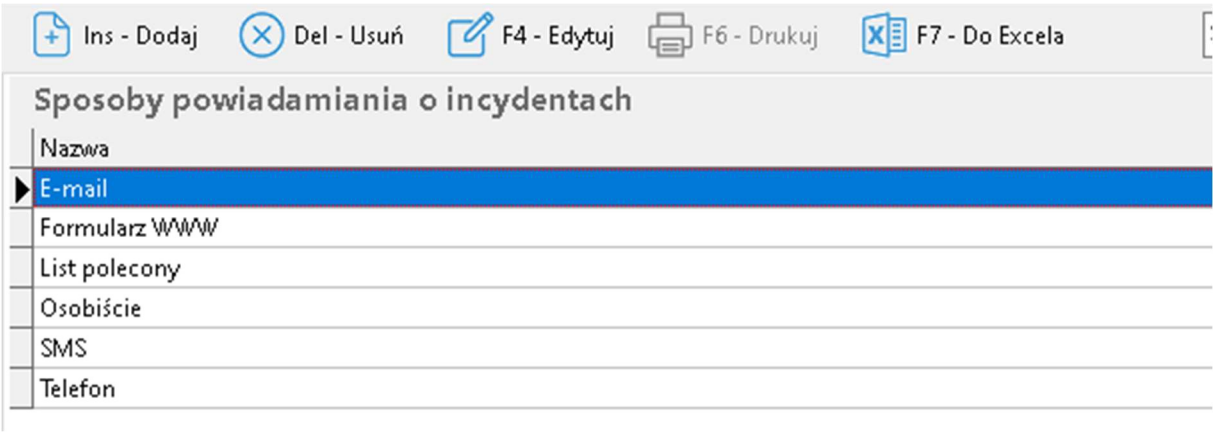
1. Dostęp do ustawień możliwy jest w zakładce Słowniki.



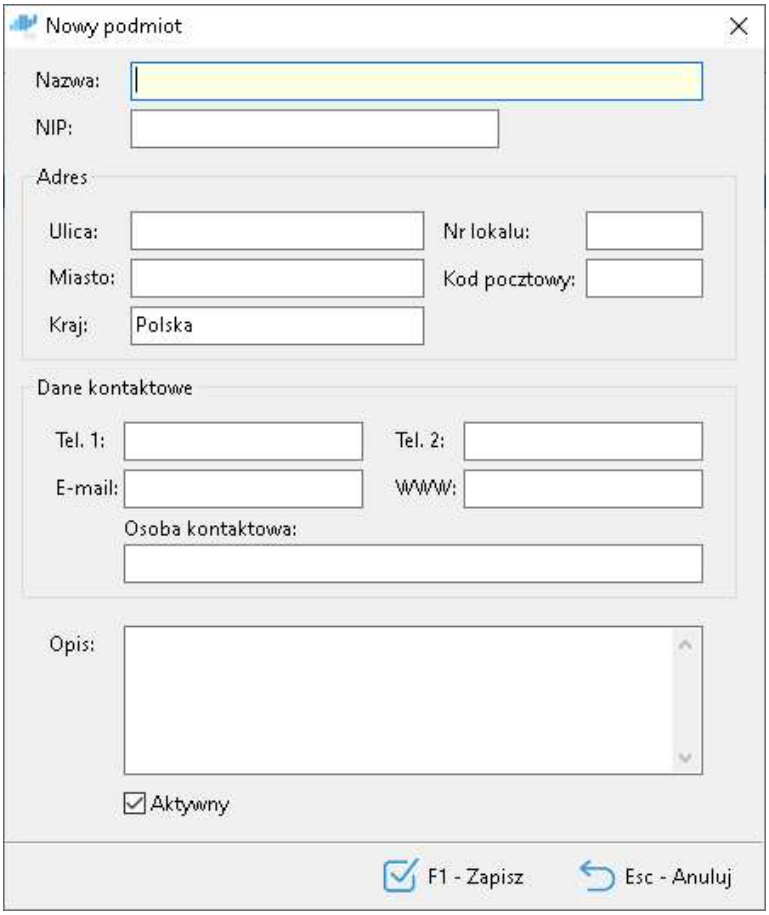
2. Rodzaje zgłoszeń.
   Na tej zakładce administrator może zdefiniować własne rodzaje zgłoszeń. Funkcja ta pozwala na dostosowanie funkcji zarządzania incydentami zgodnie z obowiązującymi zasadami.



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.

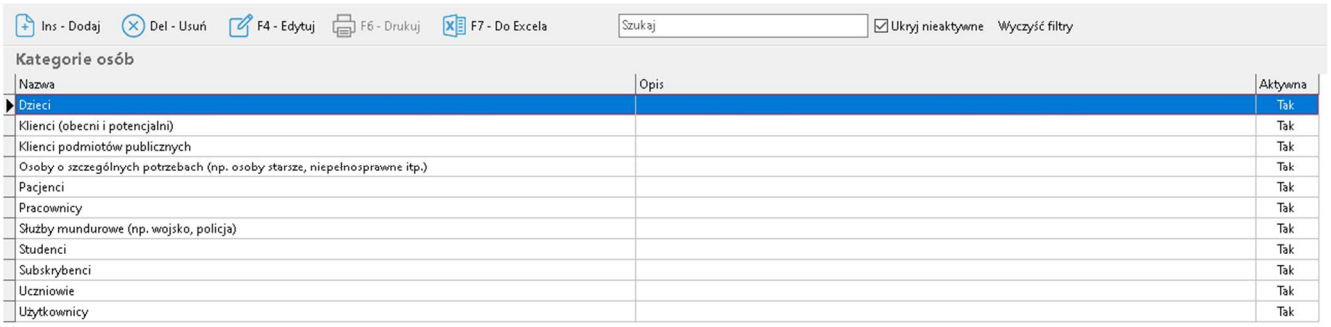


5. Kategorie danych.
   Ta funkcja pozwala na zdefiniowanie kategorii danych osobowych przetwarzanych w firmie.

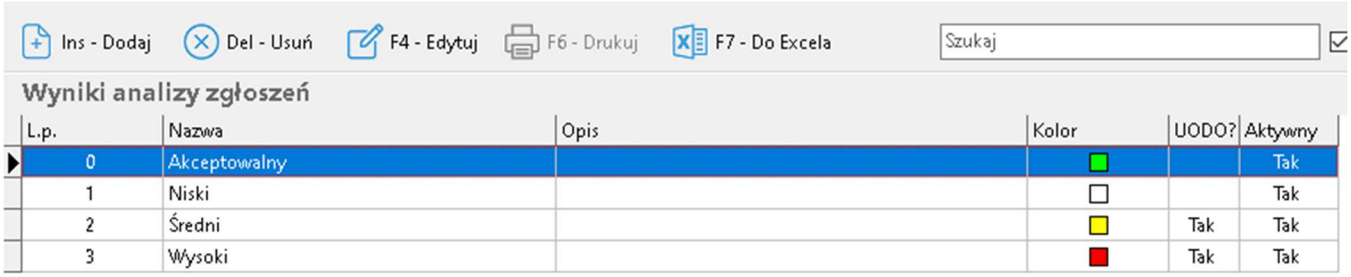
Kategorie danych

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.

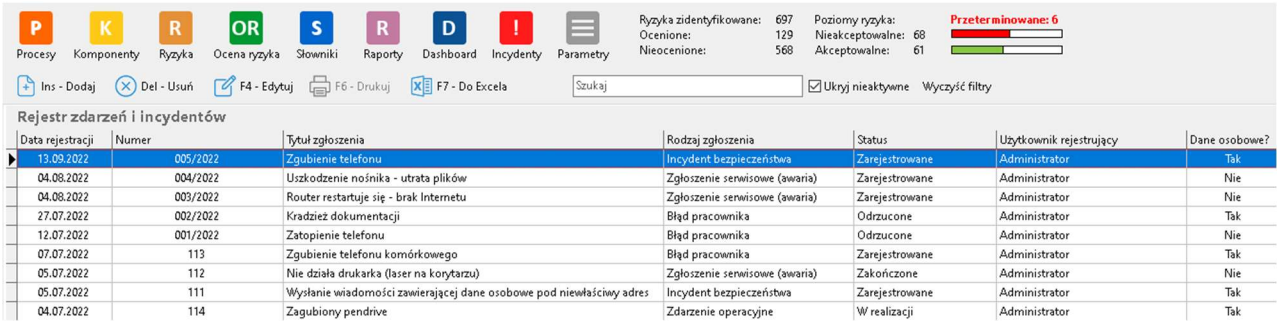


7. Wyniki analizy zgłoszeń.
   Program umożliwia budowanie własnych progów oceny incydentu. W przypadku wprowadzania zmian należy zdefiniować zasadę zgłaszania naruszenia danych osobowych do UODO.

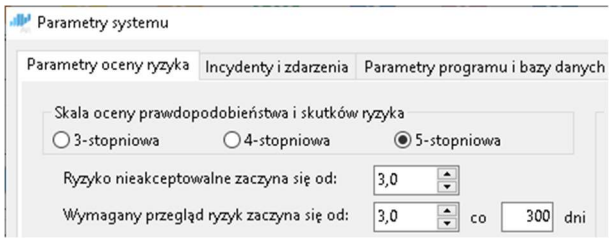


Rejestracja incydentu.

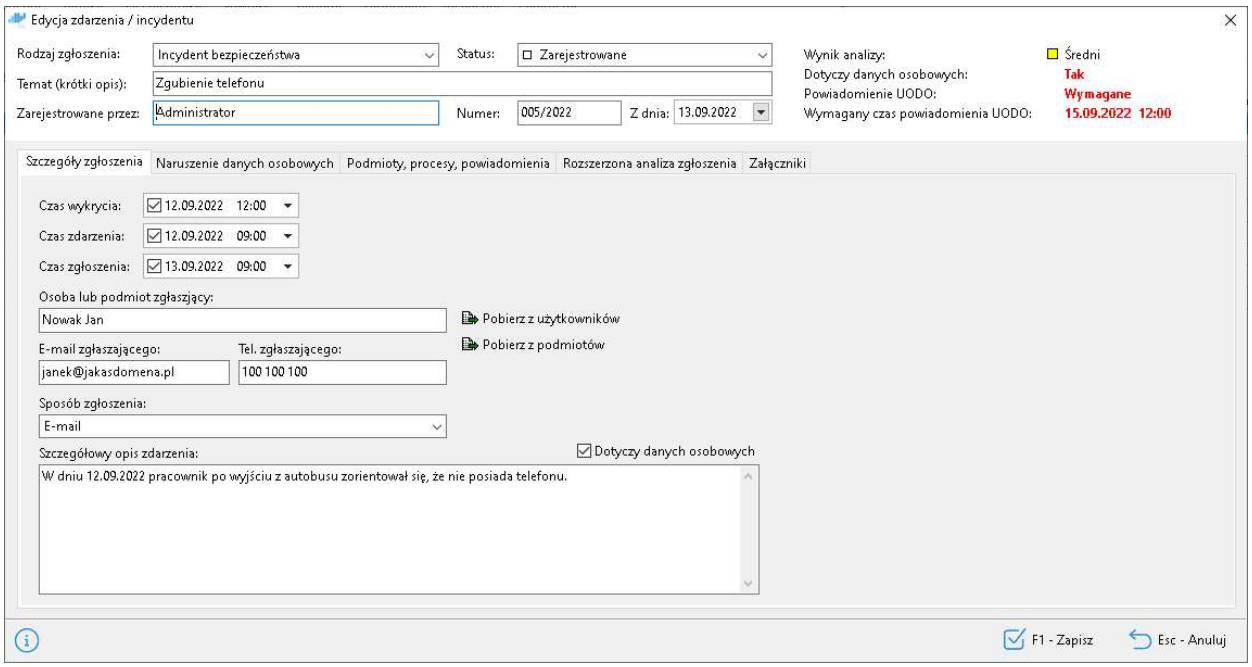
1. Po otwarciu zakładki Incydenty wchodzimy w rejestr incydentów.



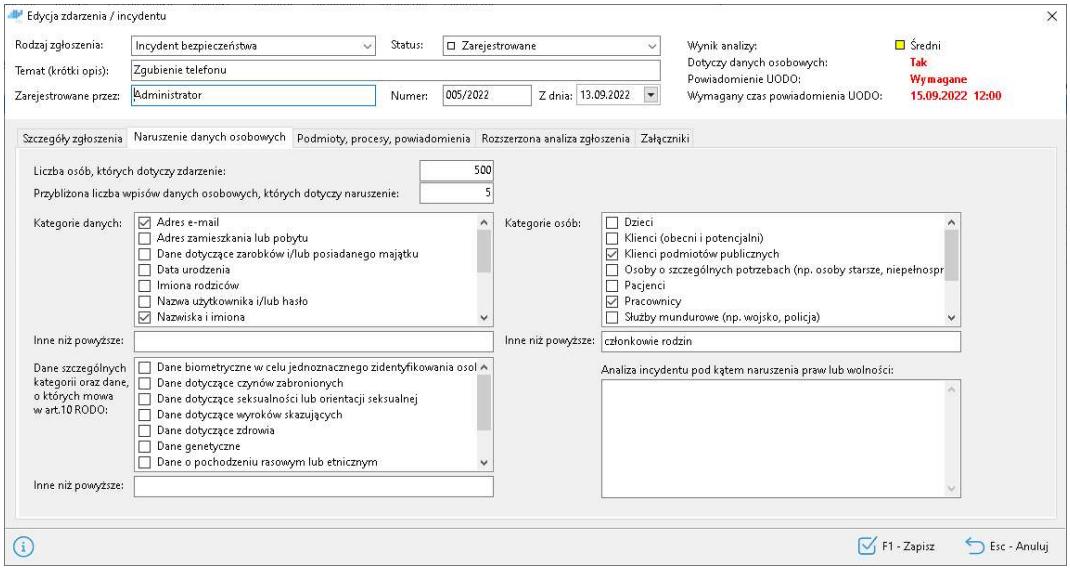
2. Na zakładce szczegóły zgłoszenia zgłaszający definiuje:
   - Rodzaj zgłoszenia.
   - Status.
   - Temat (krótki opis).
   - Informację o osobie rejestrującej zdarzenie.
   - Numer zgłoszenia (system umożliwia automatyczną numerację oraz numerację ręczną) zmiany definiuje się w Parametrach programu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



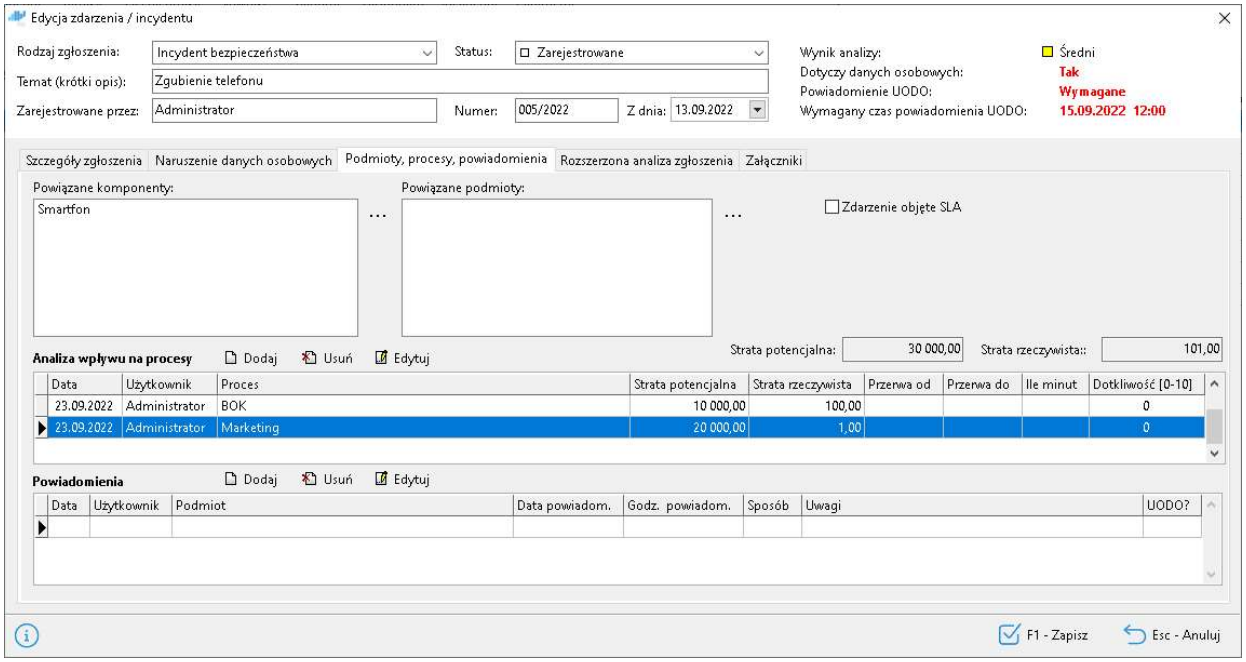
   - Czas wykrycia zdarzenia oraz zgłoszenia.
   - Informację o osobie lub podmiocie zgłaszającym (można wpisać ręcznie lub pobrać z bazy użytkowników i podmiotów).
   - Adres e-mail oraz telefon zgłaszającego.
   - Szczegółowy opis zdarzenia.
   - Checkbox dane osobowe wykorzystywany w przypadku, gdy zdarzenie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



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.



5. Analiza wpływu na procesy.
   Zakładka służy do określenia strat potencjalnych oraz strat rzeczywistych oraz określenie zakłócenia działania procesów w tym objętych umowami SLA.