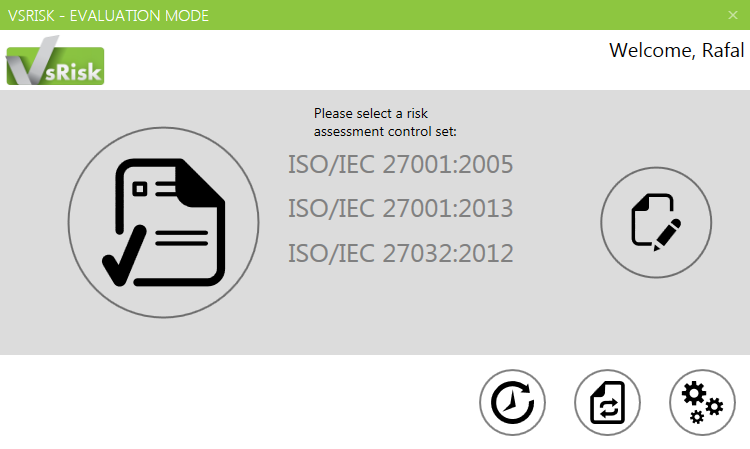
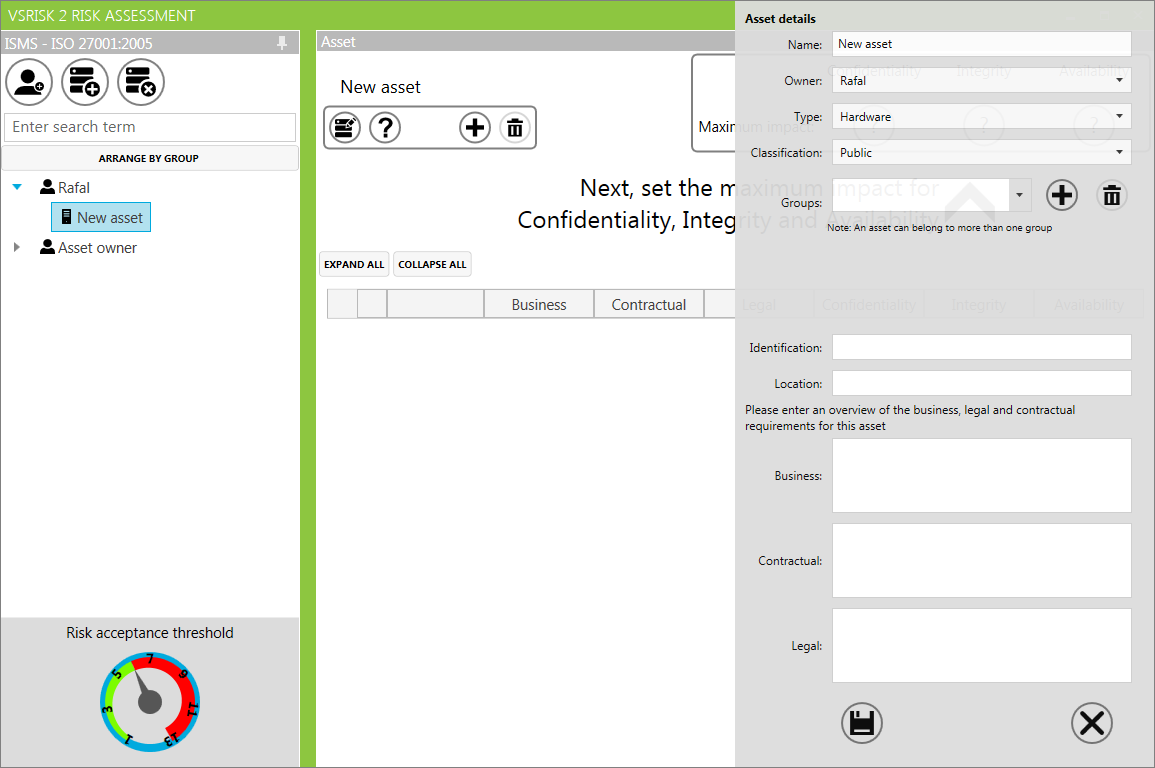
**vsRisk™ Standalone - firmy Vigilant software**

Program vsRisk to proste w obsłudze i intuicyjne narzędzie do przeprowadzenia audytów bezpieczeństwa w firmach i korporacjach. Narzędzie to obsługuje normy: ISO/IEC 27001:2005, ISO/IEC 27001:2012 oraz ISO/IEC 27001:2013. Jest to narzędzie desktopowe, które działa pod kontrolą systemu Microsoft Windows. Narzędzie to umożliwia korzystanie z lokalnej bazy danych jak i zainstalowanej na zdalnym serwerze. Instalacja na zdalnym serwerze pozwala na wypełnianie informacji dotyczących ryzyka zasobów przez ich właścicieli na osobnym komputerze bez potrzeby synchronizacji danych. Jest to duże ułatwienie ponieważ wszyscy właściciele zasobów ni e muszą korzystać fizycznie z jednej maszyny by przekazać informacje dotyczące swoich zasobów. To z pewnością przyczynia się do przyspieszenia procesu przeprowadzania audytu.

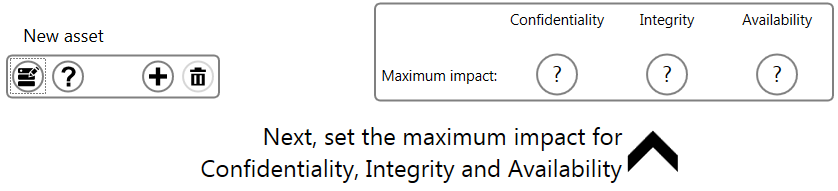
Narzędzie jest bardzo intuicyjne w obsłudze. Po uruchomieniu programu pojawia się okno które umożliwia wybór opcji programu takich jak: utworzenie raportów (Reports), szacowanie ryzyka (Risk assessment), import lub eksport (Import / eksport), konfiguracje aplikacji (Settings), podgląd historii wykonywanych operacji (History).



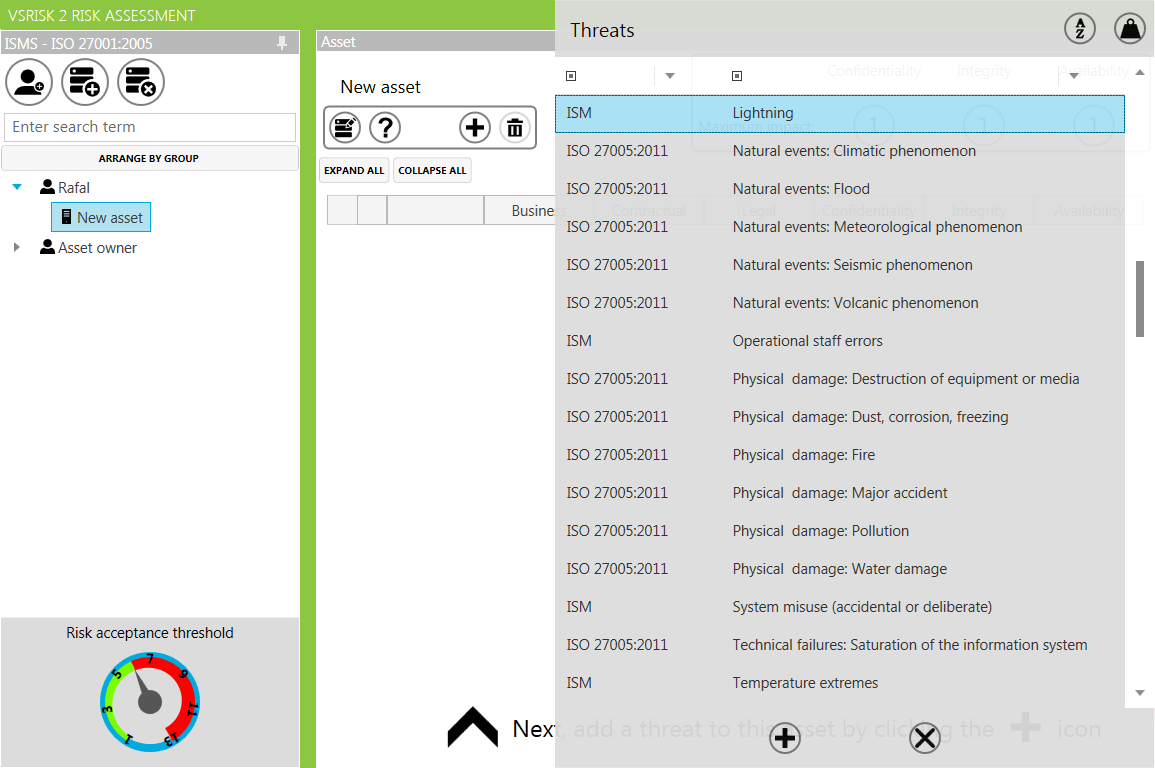
Po wybraniu opcji "Risk assessment" pojawia się nowe okno do konfiguracji zasobów, przypisywania im zagrożeń oraz podatności. W lewej części okna można dodawać nowe zasoby (Assets). Każdy dodany zasób można skonfigurować. Opcje dostępne to m.in. nazwa (Name), Właściciel (Owner), typ (Type). Dostępne typy to Hardware, Software, IP, Information/Database, Service, People, Intangible, Process.



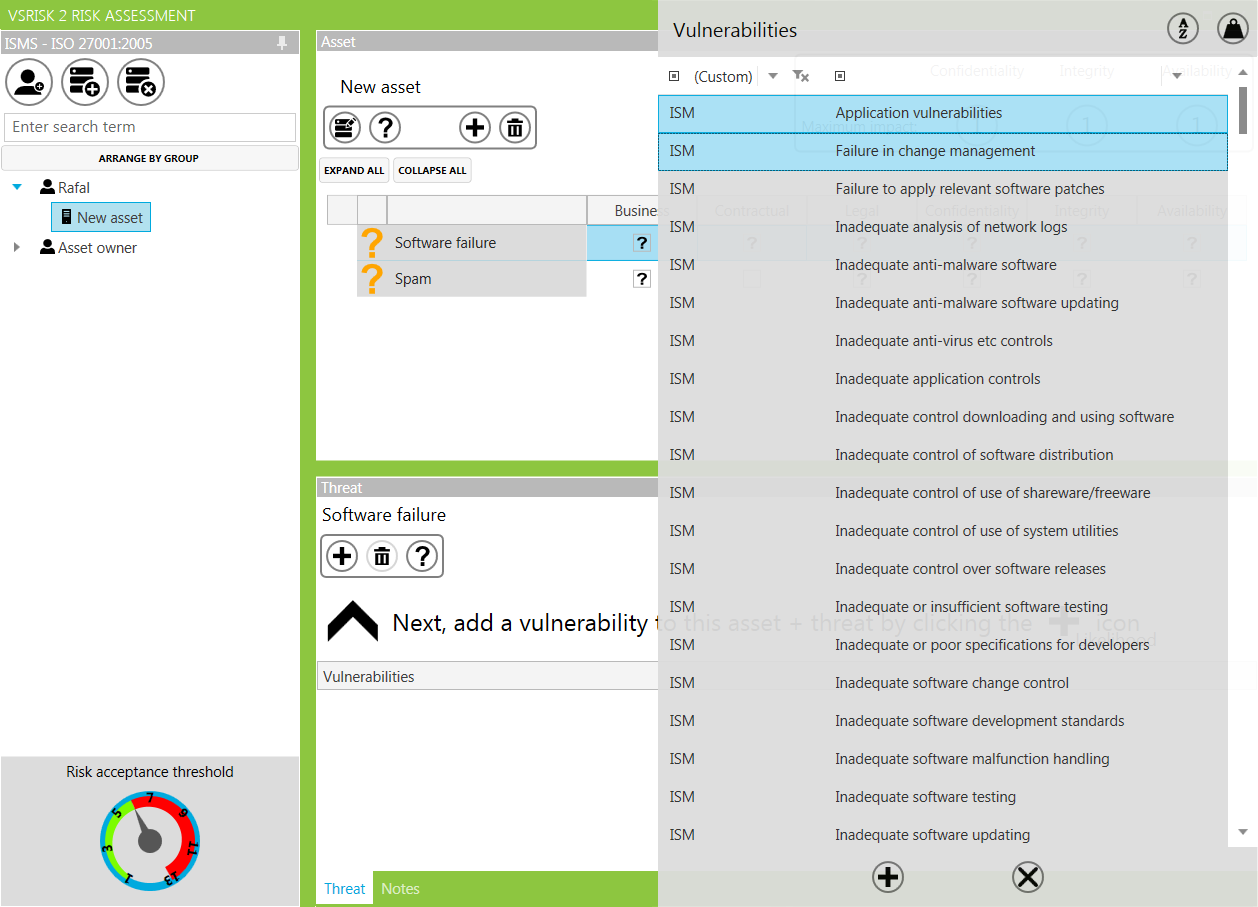
Po dodaniu i skonfigurowaniu zasobu trzeba ustawić maksymalny wpływ na poufność, integralność i dostępność. Wpływ jaki można ustawić to wartość liczbowa zawierająca się w przedziale od 1 do 7 gdzie liczba 1 to najmniejszy wpływ, a liczba 7 to największy.



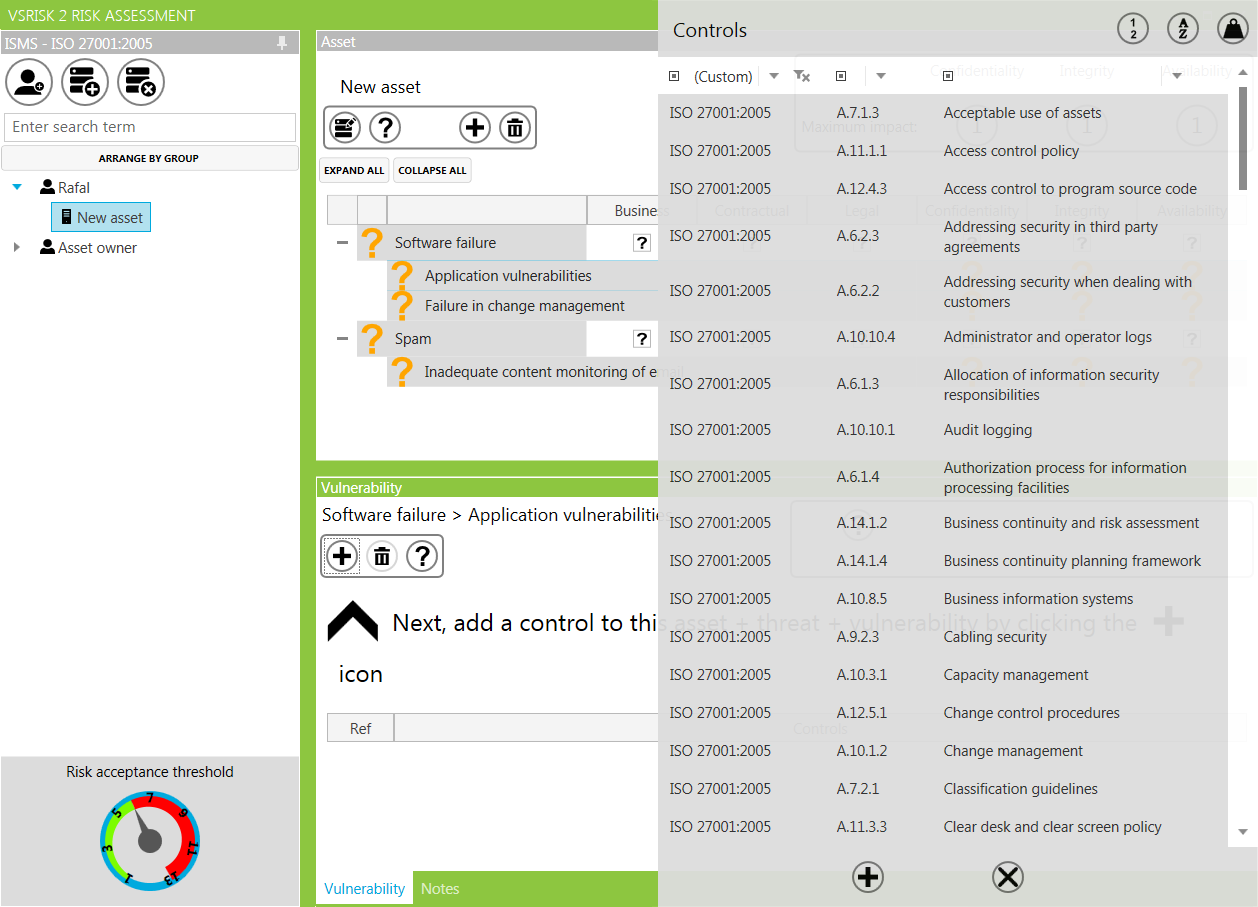
Po uzupełnieniu tych danych można dodawać zagrożenia (Threads) do nowego zasobu. Po wciśnięciu przycisku "Add thread" z prawej strony pojawi się lista możliwych zagrożeń. Należy wybrać jedno bądź kilka zagrożeń i wcisnąć przycisk "Add thread". Dzięki temu zagrożenia zostaną przypisane do bieżącego zasobu.



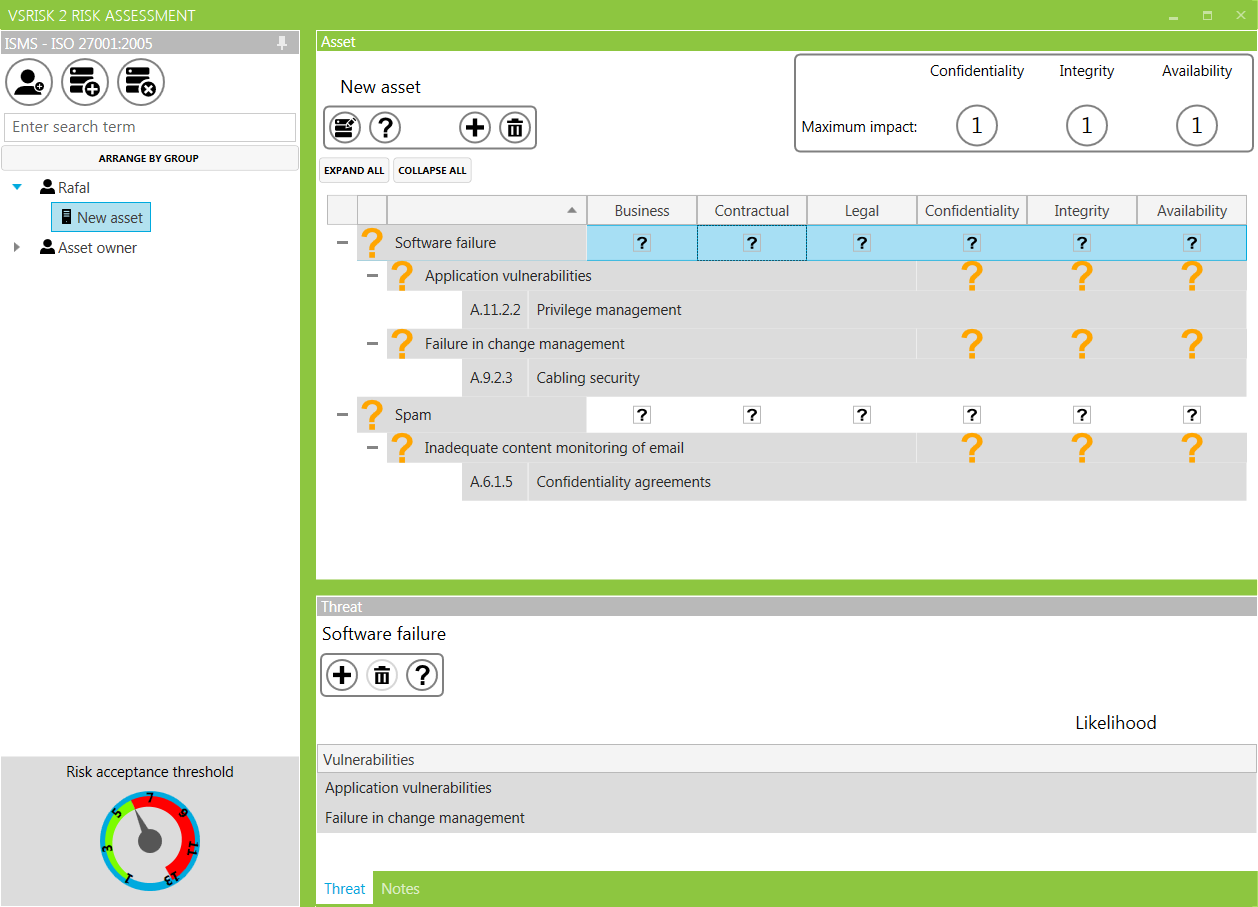
Następnie dla każdego zagrożenia należy przypisać możliwe podatności. Dodawanie nowych podatności odbywa się analogicznie jak w przypadku dodawania zagrożeń.



W ten sam sposób należy przypisać scenariusze zagrożeń do podatności.



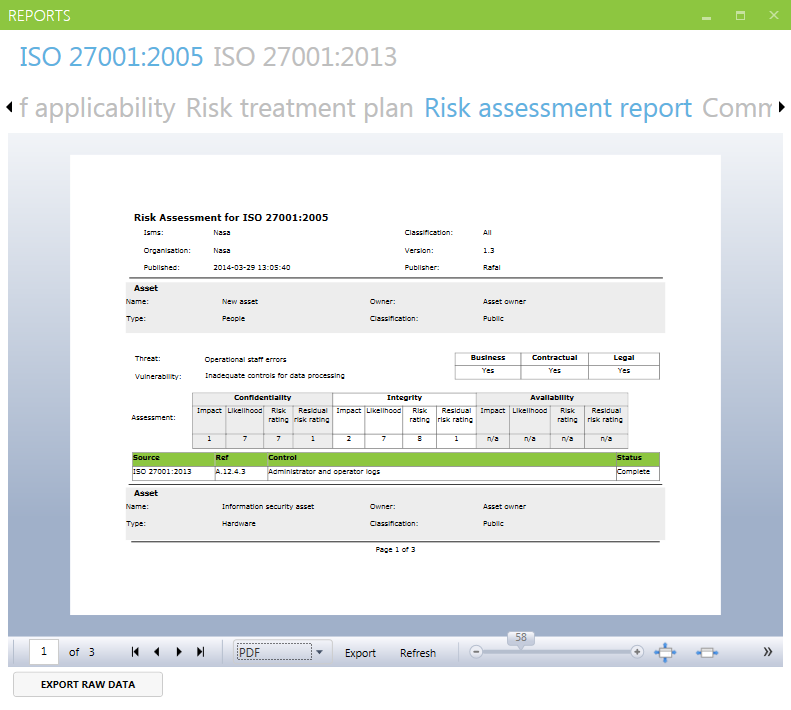
W wyniku przypisania podatności do zasobów oraz zagrożeń do podatności powstaje macierz, którą należy wypełnić.



Po wypełnieniu macierzy możliwe jest sporządzenie raportu. Funkcję raportowania można włączyć wciskając przycisk Raports w oknie głównym. Po wciśnięciu przycisku pojawiają się opcje raportów oraz dostępne normy ISO raportów.



Dostępne normy w raportowaniu to ISO:27001:2013 oraz ISO:27001:2005. Natomiast dostępne typy raportów to: Statement of applicability, Risk treatment plan, Risk assesment report, Comments report. By wygenerować raport dla stworzonej macierzy należy wybrać opcję Risk assesment report. Po wciśnięciu przycisku raport zostanie wygenerowany, który następnie można zapisać w formatach PDF, XPS, Excel 2003 oraz Excel 2007.

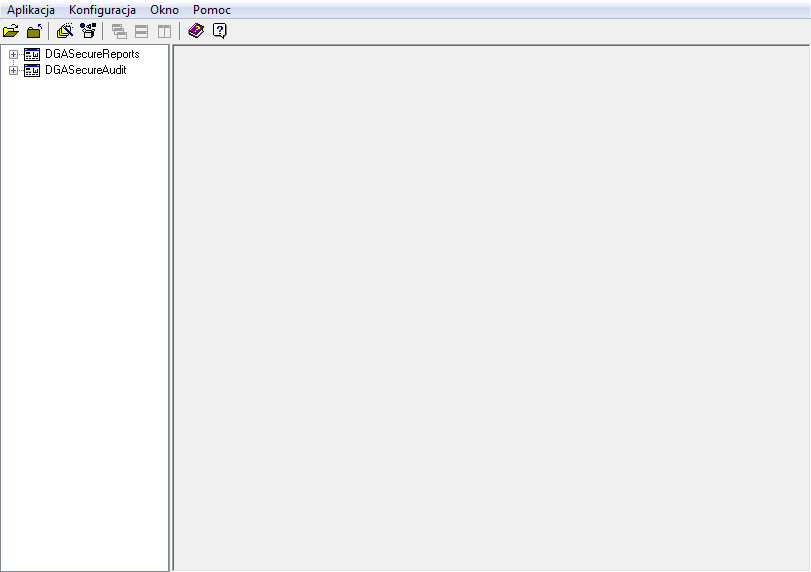


Podsumowując program vsRisk 2 jest bardzo prostym w obsłudze i intuicyjnym narzędziem. Prowadzi on użytkownika krok po kroku. Pozwala na szybkie sporządzanie audytów bezpieczeństwa. Jednak produkt ten nie jest pozbawiony wad. Jedną z nich jest duży koszt licencji. Kolejną wadą dla niektórych użytkowników może być brak wersji dla systemu operacyjnego Linux.

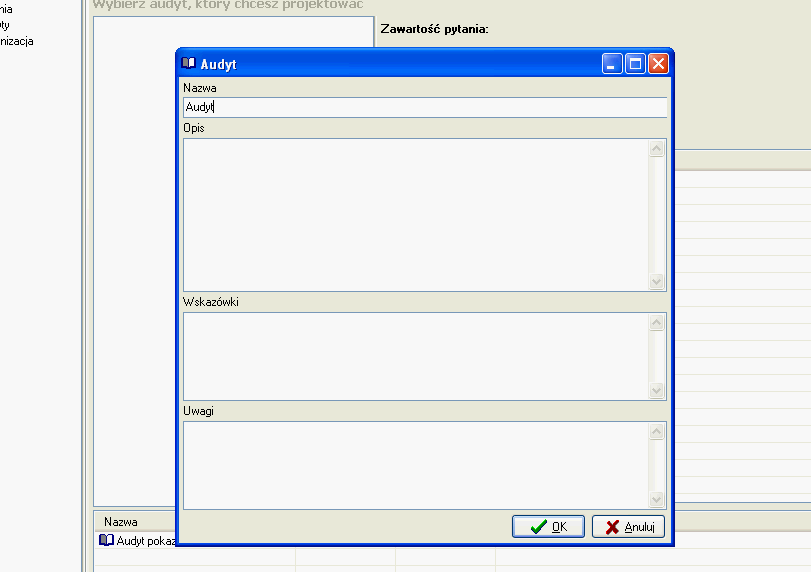
DGA Secure Audit

Oprogramowanie DGA Secure Audit pozwala na tworzenie audytów bezpieczeństwa w dwóch standardach: ISO/IEC 17799 oraz ISO/IEC 27001. Dużą zaletą prezentowanego programu jest możliwość dopasowania elementów przeprowadzanego audytu takich jak bazy pytań, struktury organizacyjnej firmy, list kontrolnych czy dostępnej skali ocen. Dzięki temu przeprowadzany audyt jest w pełni dopasowany do profilu firmy co sprawia, że przeprowadzenie audytu staje się szybsze i łatwiejsze. Użytkownik podczas projektowania audytu może wybierać z następujących list kontrolnych: ISO/IEC 17799, ISO/IEC 27001, ISO 9001, ISO 14001 i AQAP. Kolejną zaletą DGA Secure Audit jest możliwość przypisywania zadań do różnych osób, które odpowiadają za różne działy organizacji. Kolejną ważną opcją jest możliwość raportowania audytów w formie graficznej. Po przeprowadzeniu audytu zostanie wygenerowany wykres, który można dostosować do własnych potrzeb.

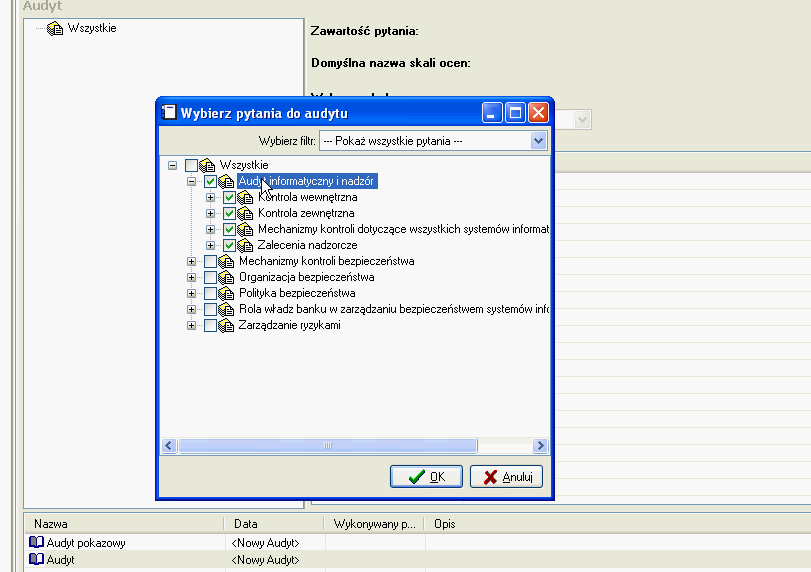
Narzędzie DGA Secure Audit z powodu dostępności wielu funkcji nie jest tak proste i intuicyjne jak w przypadku wcześniej prezentowanego vsRisk. Po uruchomieniu programu pojawia się puste okno. W menu bocznym znajduje się lista z zainstalowanymi modułami.



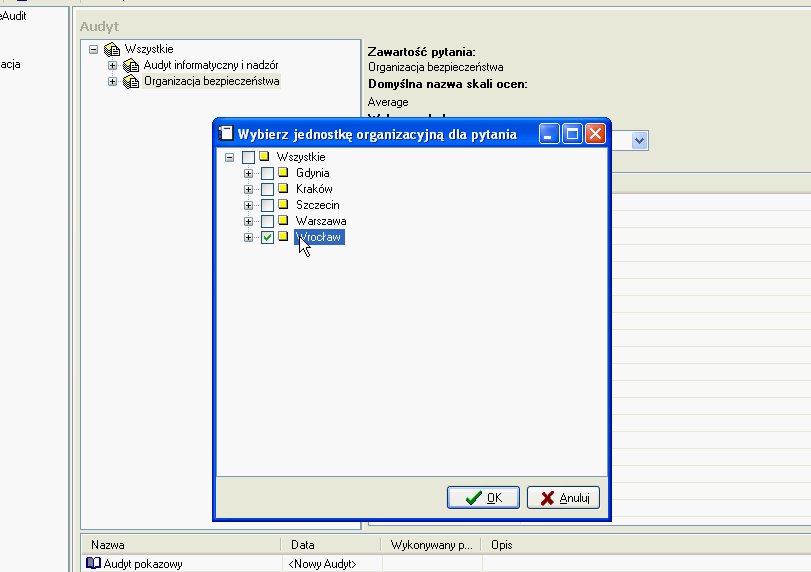
W celu przeprowadzenia audytu trzeb go najpierw zaprojektować . W tym celu należy wybrać z listy dostępnych modułów Dga Secure Audit. Z rozwijanego menu kliknąć opcję Audyty a następnie kliknąć Dodaj. W kreatorze dodawania nowego audytu można ustawić opcje takie jak: Nazwa, Opis, Wskazówki oraz Uwagi.



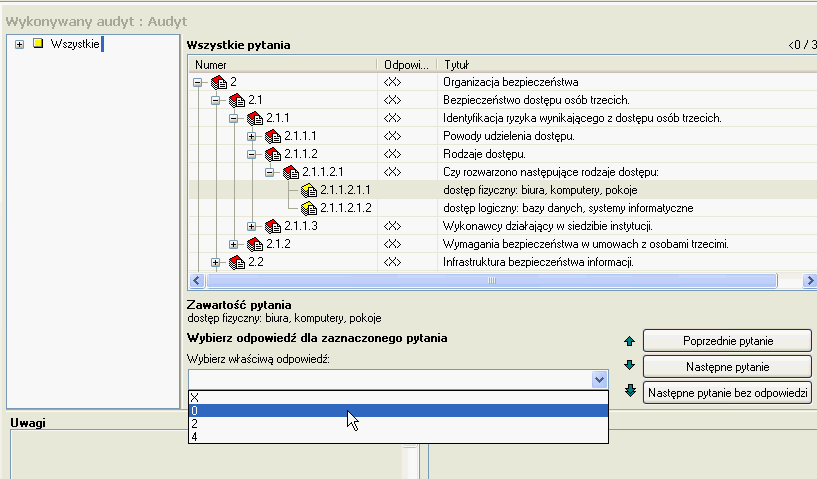
Po utworzeniu nowego audytu należy go skonfigurować. W tym celu należy przypisać pytania do tego audytu. Pytania są podzielone na kilka kategorii, należy więc wybrać jedną lub kilka kategorii, której audyt będzie dotyczyć. Do każdej kategorii bądź pytania można zdefiniować osobną skalę ocen. W den sposób określamy jakie wartości osoba przeprowadzająca audyt będzie przypisywać do pytania. Dostępny wybór zakresu odpowiedzi to: Average, Bool, Empty, Percentage, Standard, Sum, Zagrożenie.



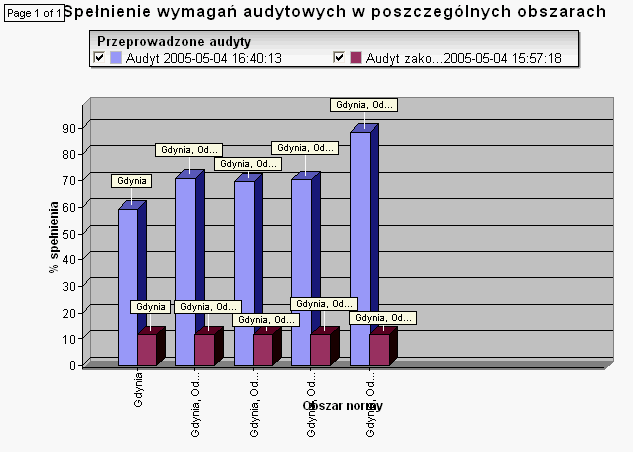
Ostatnim elementem projektowania audytu jest przypisanie jednostki organizacyjnej do kategorii pytań. Przypisana jednostka w trakcie przeprowadzania audytu będzie musiała odpowiedzieć na pytania z przypisanych do niej kategorii.



Po zaprojektowaniu audytu można go wykonać. Dzięki możliwości projektowania audytów jego wykonanie jest o wiele łatwiejsze i mniej czasochłonne. Jest ono także lepiej dostosowywane do konkretnego przypadku. Audyt odbywa się poprzez wybieranie odpowiedzi na pytania z listy możliwych odpowiedzi lub wpisywania odpowiednich wartości w polu tekstowym zależnie od wcześniej zdefiniowanego typu pytania.



Po zakończeniu wykonywania audytu program umożliwia wygenerowanie wykresu raportu. Raport może dotyczyć całego audytu lub też wybranych jednostek organizacyjnych. Wykres generowany jest w układzie dwóch współrzędnych gdzie współrzędna X to Obszar normy natomiast współrzędna Y to % spełnienia normy.



Podsumowując program DGA Secure Audit to rozbudowane narzędzie, które pozwala na wcześniejsze zaprojektowanie audytu. Powoduje to, że proces przeprowadzania audytu jest łatwiejszy a sam audyt jest bardziej dopasowany do profilu oraz organizacji firmy.

Jednak liczba dostępnych opcji sprawa, że sam program nie jest tak intuicyjny jak w przypadku wcześniej omawianego programu vsRisk i użytkownik przed rozpoczęciem pracy musi się zapoznać z instrukcją.

DGA Secure Risk