Cykl Metodyka Audytu

Wykorzystanie automatycznych narzędzi do testów i analiz w zadaniu audytowym – studium przypadku.

AUDYT WEWNĘTRZNY

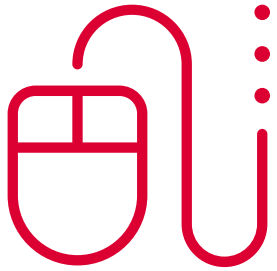
31 maja 2023 r.

Techniki audytu wykorzystujące technologię informatyczną

1220.A2 – Działając z należytą starannością zawodową audytorzy wewnętrzni muszą rozważyć możliwość użycia technik audytowych wykorzystujących technologie informatyczne oraz innych technik analizy danych

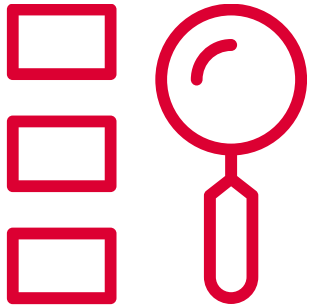
Techniki audytu wykorzystujące technologię informatyczną – Wszelkie zautomatyzowane narzędzia audytu, takie jak ogólne oprogramowanie audytowe, generatory danych testowych, skomputeryzowane programy audytowe, specjalne narzędzia audytowe i techniki audytu wspierane komputerowo (ang. CAATs – Computer Assited Audit Techniques).

Techniki audytu wykorzystujące technologię informatyczną



- Excel, Excel + VB, Excel + xlwings, Power Query,
- Power Bi, Tableau, Qlick,
- Uniwersalne oprogramowanie audytorskie (GAS – General Audit Software), np. ACL, IDEA, Arbutus, KNIME,
- Automatyzacja czynności przy użyciu skryptów lub aplikacji języków programowania np. VB, Python, Java, C++.

Informacje ogólne o zadaniu audytowym



Temat zadania zapewniającego

Ocena wdrożenia standardów w zakresie cyberbezpieczeństwa

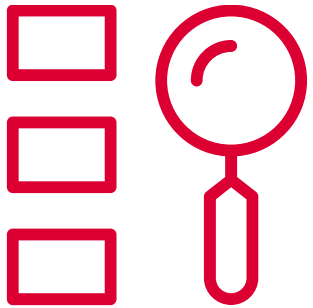
Cel zadania

Przedstawienie kierownictwu jednostki w dziale oraz Komitetowi Audytu oceny poziomu dojrzałości zarządzania w zakresie budowania odporności na cyberzagrożenia, w tym wdrożenia przez jednostki zalecanych standardów w zakresie cyberbezpieczeństwa.

Cele dodatkowe

- Identyfikacja słabości systemowych mających wpływ na odporność cyberprzestrzeni resortu sprawiedliwości;
- Identyfikacja dobrych praktyk zarządzania cyberbezpieczeństwem, wartych upowszechnienia.

Informacje ogólne o zadaniu audytowym



Źródła kryteriów oceny mechanizmów kontrolnych i poziomu dojrzałości zarządzania to przepisy prawa, wytyczne oraz dobre praktyki, w szczególności:

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2022 r. poz. 1863 ze zm.);
- Rozporządzenie Prezesa Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI … (t.j. Dz. U. z 2017 r. poz. 2247);
- Zarządzenia i wytyczne resortowe w badanym obszarze.

Ocena dojrzałości zarządzania

Kryteria oceny wraz ze sposobem klasyfikowania wyników dla poszczególnych kryteriów służyły dokonaniu oceny dojrzałości zarządzania w 4-stopniowej skali na poziomie całego zadania i każdego z 4 obiektów audytu.

Informacje ogólne o zadaniu audytowym

Zakres podmiotowy zadania

Czynności audytowe w pełnym zakresie objęły **88** jednostek w dziale oraz **66** jednostek nadzorowanych w zakresie częściowym (obiekt A). Łącznie audytem cyberbezpieczeństwa objęto **154** jednostki.

Informacje ogólne o zadaniu audytowym

<u>Zakres przedmiotowy – obiekty audytu:</u>

A. Weryfikacja wdrożenia 5 rekomendowanych standardów cyberbezpieczeństwa (waga 42%):

- łącze zapasowe dostępu do sieci resortowej,
- uwierzytelnianie połączeń zdalnych,
- podłączenie systemów pomocniczych do sieci jednostki,
- przejście na system operacyjny Windows 10,
- używanie innych systemów w domenie ksiąg wieczystych.

Informacje ogólne o zadaniu audytowym

<u>Zakres przedmiotowy – obiekty audytu:</u>

B. Stosowanie innych dobrych praktyk w zakresie cyberbezpieczeństwa (waga 20%):

- szyfrowanie dokumentów wysyłanych pocztą elektroniczną,
- bezpieczeństwo i publikacja danych na stronie internetowej,
- aktualizacja systemów operacyjnych i oprogramowania antywirusowego,
- bezpieczeństwo urządzeń przenośnych (pendrive, laptop itp.),
- inwentaryzacja sprzętu i oprogramowania (w rozumieniu Krajowych Ram Interoperacyjności).

Informacje ogólne o zadaniu audytowym

<u>Zakres przedmiotowy – obiekty audytu:</u>

C. Budowa odporności na cyberzagrożenia (waga 28%):

- Kształtowanie świadomości pracowników, usługodawców i interesantów jednostki w zakresie cyberzagrożeń (szkolenia, działania informacyjne):

✓ **przeprowadzenie testu wiedzy (ankietowego),**

✓ **przeprowadzenie testu phishingowego.**

Informacje ogólne o zadaniu audytowym

<u>Zakres przedmiotowy – obiekty audytu:</u>

D. Zarządzania incydentami cyberbezpieczeństwa (waga 10%):

- Organizacja zarządzania incydentami,
- Obsługa incydentów cyberbezpieczeństwa.

Cel testu pozorującego atak phishingowy

Przeprowadzenie testu pozorującego atak phishingowy miało na celu sprawdzenie przygotowania jednostek co do odporności na podatność związaną z niską świadomością pracowników jednostek i osób świadczących usługi zewnętrzne w zakresie cyberbezpieczeństwa (m.in. podatność na ataki socjotechniczne, phishingowe itp.).

Phishing to rodzaj cyberataku, podczas którego cyberprzestępca próbuje wyłudzić od ofiary poufne informacje. Jest to najpopularniejszy rodzaj cyberataku, którego celem jest np. kradzież loginów, numerów kart kredytowych i rachunków bankowych czy wrażliwych informacji firmowych.

Ankieta - test wiedzy

Narzędzia:

Hosting: acl.org.pl

Technologia strony: php
Baza danych: MySql

Konsola administratora: Python

Koszt = 0 zł

Ankieta - test wiedzy

Założenia:

1. Test był przeprowadzony w okresie przed wykonaniem testu phishingowego.
2. Każdy audytor w jednostce otrzymał link do anonimowego testu dla swojej jednostki oraz link do wyników.
3. Test mógł być przeprowadzony na danym komputerze jeden raz.
4. Po upłynięciu terminu jego aktywności ulegał deaktywacji.
5. Test posiadał 20 takich samych pytań, jednakże każde wywołanie ustawiało w losowo kolejność pytań oraz odpowiedzi.
6. Wyniki każdy z audytorów odczytywał samodzielnie.
7. Punktacja:

   wynik >= 90% - 5 pkt
   wynik >= 80% - 4 pkt
   wynik >= 70% - 3 pkt
   wynik >= 60% - 2 pkt
   wynik >= 50% - 1 pkt
   wynik < 50% - 0 pkt

Test phishingowy

Narzędzia:

Hosting: msqov.pl
Server: Linux Ubuntu 20.04,
Server www: Apache/2.4.41
Server poczty: Postfix
Baza danych: MySQL 8.0.20-0ubuntu 20.04.1
Php: PHP 7.4.3
Python 3.8.2

Konsola administratora: Python

Koszt = 0 zł

Test phishingowy

Założenia:

1. Dane adresów mailowych pracowników sądów są zbierane i przetwarzane wyłącznie przez pracowników Samodzielnego Stanowiska do spraw Audytu Wewnętrznego w Biurze Ministra (w skrócie SSAW).

2. Serwer, na którym będą zbierane wyniki zachowań pracowników sądów jest umiejscowiony w infrastrukturze Sądu Apelacyjnego w Krakowie. Obejmuje on środowisko Linux wraz z serwerem www, bazą danych MySQL oraz Python. Będzie on udostępniony publicznie wyłącznie na okres prowadzenia testu.

3. Dane gromadzone na serwerze są zaszyfrowane, zatem nie ma możliwości poznania zapisanych danych mailowych przez inne nieuprawnione osoby.

Test phishingowy

Scenariusz:

1. Pracownicy SSAW zbierają formularze w formacie plików Excel od audytorów poszczególnych sądów, zawierające adresy mailowe pracowników wraz z ich przypisaniem do poszczególnych komórek organizacyjnych. Na podstawie tych danych sporządzana jest jedna lub kilka list w przygotowanym formacie do wgrania na serwer.
2. Dane wgrywane na serwer są przez SSAW są w zaszyfrowanym w pliku, zatem wgrywanie ich drogą elektroniczną na serwer jest zabezpieczone przed nieuprawnionym dostępem. Serwer bowiem wykorzystywany do celów testu celowo operuje wyłącznie na połączeniach „http”, aby dać szansę uczestnikom testu na właściwe zachowanie.
3. Wgrywanie danych na serwer odbywa się poprzez przygotowaną stronę www. Dostęp do panelu, gdzie następuje przesłanie pliku z zaszyfrowanymi danymi, jest możliwy po podaniu jednorazowego hasła. Dane po przesłaniu są przy pomocy skryptów Python przetwarzane poza środowiskiem serwera www i umieszczane w bazie danych a następnie na ich podstawie przygotowywane unikatowe linki dla każdego adresu email.

Test phishingowy

Scenariusz:

4. Wysyłkę spreparowanych maili do poszczególnych adresów mailowych dokona oprogramowanie serwera, bez udziału osób zewnętrznych. Moment inicjacji wysyłki będzie wybrany przez SSAW i a sama wysyłka będzie rozpoczęta poprzez wydanie odpowiedniego polecenia przez przygotowaną stronę internetową. Dostęp do panelu wyzwalającego wysyłkę jest również możliwy tylko po podaniu jednorazowego hasła.
5. Obsługa procesu wgrywania danych i wysyłki maili nie wymaga ze strony SSAW żadnego dodatkowego oprogramowania, oprócz przeglądarki internetowej oraz posiadania haseł dostępowych do panelu wgrywania danych i wysyłki. Wyjątkiem jest jedynie aplikacja do zaszyfrowania zawartych danych w pliku tekstowym.
6. Po uruchomieniu testu, dane odnośnie czynności na fałszywej stronie internetowej są logowane w bazie danych, nie zawierają jednak żadnych danych osobowych. Nie są przesyłane na serwer podawane przez poszczególne osoby hasła.

Test phishingowy

Scenariusz:

7. Po zakończeniu testu każdy z audytorów wykonujący zadanie audytowe w poszczególnych sądach otrzyma mailem zbiorczą informację dotyczącą zachowań pracowników audytowanego sądu w podziale na komórki organizacyjne. Będzie ona zawierać informacje o ilości ogółem przesłanych maili; ilości wejść na fałszywą stronę; ilości osób, które takich wejść dokonały; ilości poprawnych i niepoprawnych logowań oraz ilości osób, które je dokonały. Wyniki nie będą umożliwiały identyfikacji zachowań poszczególnych osób, lecz wyłącznie syntetyczne dane ogólne.

Test phishingowy

Zrzut poszczególnych elementów projektowanego systemu:

1) wejście do panelu wgrywania danych/uruchamiania startu wysyłki maili:

Hasło:

Loguj

2) panel wgrywania danych

Wysyłanie pliku z zaszyfrowanymi danymi mailowymi

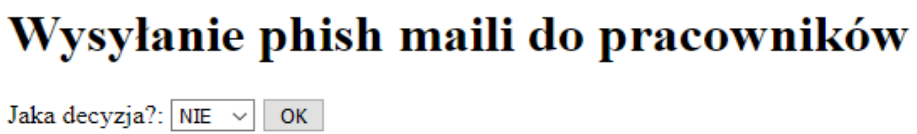
Przeglądaj... SA_Osoby_crypted.txt Wyślij

Dokonano transferu pliku do katalogu.
Wczytano dane do bazy: 2 szt. sądów, w tym nowe: 2 szt., ogółem 4 szt. osób, w tym nowych 4 szt.
Usunieto plik.
Aktywowano 4 szt. pracowników.

Test phishingowy

Zrzut poszczególnych elementów projektowanego systemu:

3) panel uruchamiania startu wysyłki maili:



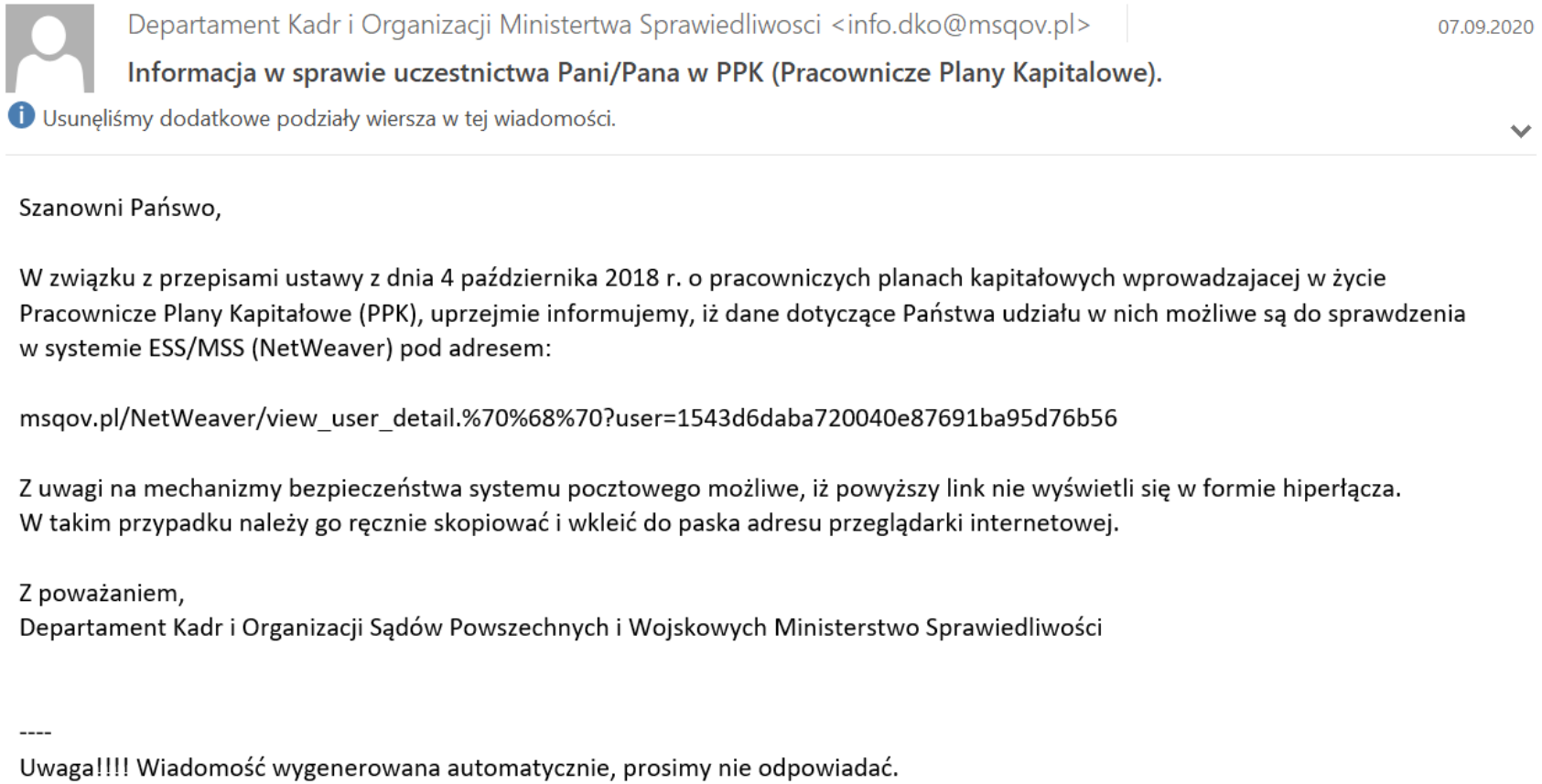
Test phishingowy

Zrzut poszczególnych elementów projektowanego systemu:

4) fałszywa strona:

Test phishingowy

Przykładowy mail:



Departament Kadr i Organizacji Ministertwa Sprawiedliwosci <info.dko@msqov.pl> 07.09.2020

Informacja w sprawie uczestnictwa Pani/Pana w PPK (Pracownicze Plany Kapitalowe).

Usunęliśmy dodatkowe podziały wiersza w tej wiadomości.

Szanowni Pańswo,

W związku z przepisami ustawy z dnia 4 października 2018 r. o pracowniczych planach kapitałowych wprowadzajacej w życie Pracownicze Plany Kapitałowe (PPK), uprzejmie informujemy, iż dane dotyczące Państwa udziału w nich możliwe są do sprawdzenia w systemie ESS/MSS (NetWeaver) pod adresem:

msqov.pl/NetWeaver/view_user_detail.%70%68%70?user=1543d6daba720040e87691ba95d76b56

Z uwagi na mechanizmy bezpieczeństwa systemu pocztowego możliwe, iż powyższy link nie wyświetli się w formie hiperłącza.
W takim przypadku należy go ręcznie skopiować i wkleić do paska adresu przeglądarki internetowej.

Z poważaniem,
Departament Kadr i Organizacji Sądów Powszechnych i Wojskowych Ministerstwo Sprawiedliwości

---
Uwaga!!!! Wiadomość wygenerowana automatycznie, prosimy nie odpowiadać.

Test phishingowy

Zasady logowania wyników:

1. **Wejścia na fałszywą stronę.**
2. **Próba zalogowania się.**
3. **Próba zalogowania się poprawnie skonstruowanym loginem + niepuste hasło.**

Wyniki:

Wysłano 19.344 maile do 81 jednostek,

Wejść na stronę: 2.106 z 74 jednostek,

Próby logowania się: 725 szt.

Próby logowania się poprawnym loginem: 586 szt.

Test phishingowy

Szanowni Państwo,

W dniu 07.09.2020 r. otrzymaliście Państwo na swoje skrzynki pocztowe wiadomość zatytułowaną: „Informacja w sprawie uczestnictwa Pani/Pana w PPK (Pracownicze Plany Kapitałowe).”
Wiadomość ta była fałszywa i mogła być była próbą wyłudzenia danych logowania do systemu informatycznego. Informujemy, iż próba ta była kontrolowanym atakiem phishingowym prowadzonym przez audytorów wewnętrznych (sądów powszechnych i MS) we współpracy i pod nadzorem Biura Cyberbezpieczeństwa Ministerstwa Sprawiedliwości. Miała ona na celu sprawdzenie czujności pracowników i ich odporności na cyber zagrożenia. Stanowiła ona jeden z testów prowadzonych w ramach audytu w zakresie cyberbezpieczeństwa w sądach powszechnych.

Jeśli ta wiadomość została przez Państwa zignorowana lub przekazana do odpowiednich osób zajmujących się cyberbezpieczeństwem w Sądzie, to oznacza, iż zachowaliście się Państwo prawidłowo.
W przypadku, gdy ktoś podjął działania, do których zachęcała treść wiadomości, tj. wszedł na fałszywą stronę i/lub próbował się zalogować to oznacza, iż nie zachował właściwej czujności i dał się oszukać.
W otrzymanej wiadomości były zawarte elementy, które powinny wskazywać odbiorcy próbę oszustwa:

1) niewłaściwy adres nadawcy: info.dko@msqov.pl – w nazwie domeny brak jest kropki oraz litera „g” w „gov” została zastąpiona literką „q”. Adres właściwy winien posiadać domenę „ms.gov.pl”
2) błędy literowe w temacie maila i samej jego treści – przykładowo:

Informacja w sprawie uczestnictwa Pani/Pana w PPK (Pracownicze Plany Kapitalowe).

Test phishingowy

Departament Kadr i Organizacji Ministertwa Sprawiedliwosci <info.dko@msqov.pl>

Szanowni Państwo,
W związku z przepisami ustawy z dnia 4 października 2018 r. o pracowniczych p
możliwe są do sprawdzenia w systemie ESS/MSS (NetWeaver) pod adresem:

3) podano łącze do strony internetowej w formie tekstowej z prośbą o wklejenie do paska adresu przeglądarki internetowej – jest to działanie niestandardowe i podejrzane

Gdyby był to prawdziwy atak phishingowy, atakujący mógłby wejść w posiadanie Państwa danych dostępowych do systemów oraz wykorzystać je do ataków na systemy sądowe oraz próbować zainfekować Państwa komputery (poprzez umieszczenie złośliwego kodu na fałszywej stronie internetowej).
W tym przypadku nic takiego nie miało miejsca, żadne dane nie zostały ujawnione (nie pozyskano żadnych haseł - nie wymagają one zatem zmiany), a cała akcja miała charakter wyłącznie edukacyjny. Proszę zatem pamiętać o codziennie występujących zagrożeniach związanych z korzystaniem z mediów elektronicznych, w tym poczty elektronicznej.

Z upoważnienia Pana Jana Kostrzewy Dyrektora Biura Cyberbezpieczeństwa MS,

Narzędzia wspomagające audytora

Narzędzia wspomagające audytora

Narzędzia wspomagające audytora

Korzyści z wykorzystania:

- szybkie realizacje analiz,
- skuteczność w wykrywaniu niezgodności/potwierdzaniu zgodności,
- ograniczenie czasu na przegląd analityczny, koncentracja na sprawach wymagających przeglądu dokumentacji,
- jesteśmy pewni, że otrzymaliśmy 100% danych,
- jesteśmy niezależni od formatów danych otrzymanych,
- automatyzacja powtarzalnych czynności,
- obiektywność wyników otrzymanych w wyniku analiz elektronicznych,
- w wielu przypadkach badamy 100% populacji,
- dokonujemy losowania w populacji ograniczonej typowaniem zakresów o największym prawdopodobieństwie występowania nieprawidłowości.

Narzędzia wspomagające audytora

Dobry audytor to człowiek leniwy ☺

Narzędzia wspomagające audytora (by me ☺)

analityczne:

- MS Excel, MS Excel + vb, MS Excel + xlwings
- ACL, IDEA, Arbutus Analyzer, KNIME
- Python

automatyzujące pracę:

- Visual Basic
- AutoIt
- AutoHotKey
- Python

wizualizacja danych:

- Excel
- PowerBI, Qlick, Tableau
- R + Shiny

dla audytu ciągłego:

- Windows (Harmonogram zadań)
- ACL AX Serwer, Arbutus Serwer
- Python
- PowerBI

coś do rysowania?

- MS Visio
- draw.io

Narzędzia wspomagające audytora (by me ☺)

Gdzie szukać informacji?

- **ACL - https://www.diligent.com/acl-analytics/**
- **IDEA - https://www.caseware.com/ca/products/idea**
- **Arbutus Analyzer – https://www.arbutussoftware.com/en/home**
- **KNIME - https://www.knime.com**
- **Python - https://www.python.org**
- **AutoIt - https://www.autoitscript.com/site**
- **PowerBI - https://powerbi.microsoft.com**
- **Tableau - https://www.tableau.com**
- **Qlick - https://www.qlik.com**

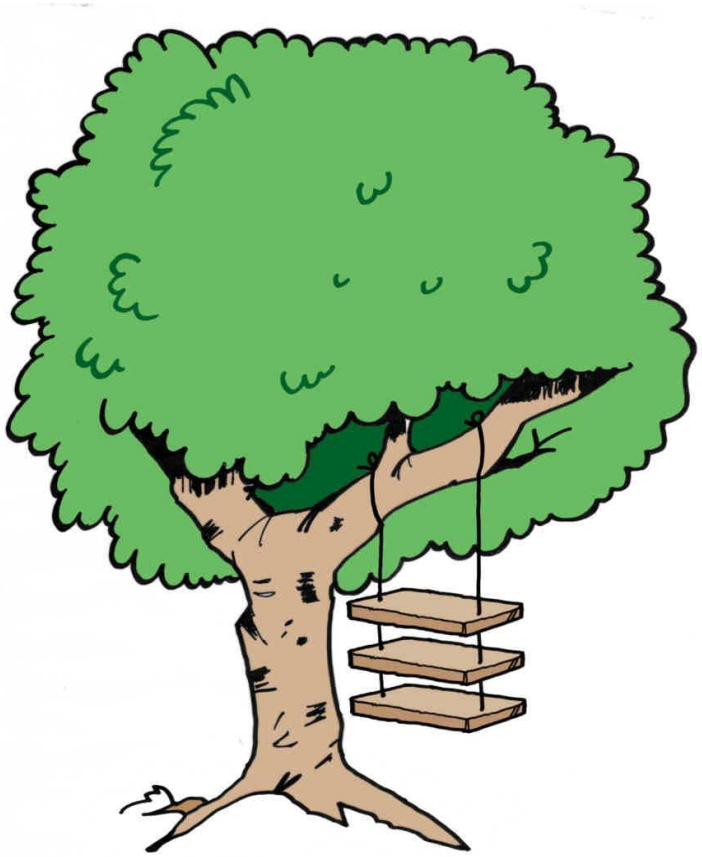
Narzędzia wspomagające audytora

Jak rozmawiać z IT???

Narzędzia wspomagające audytora

Jak rozmawiać z IT???

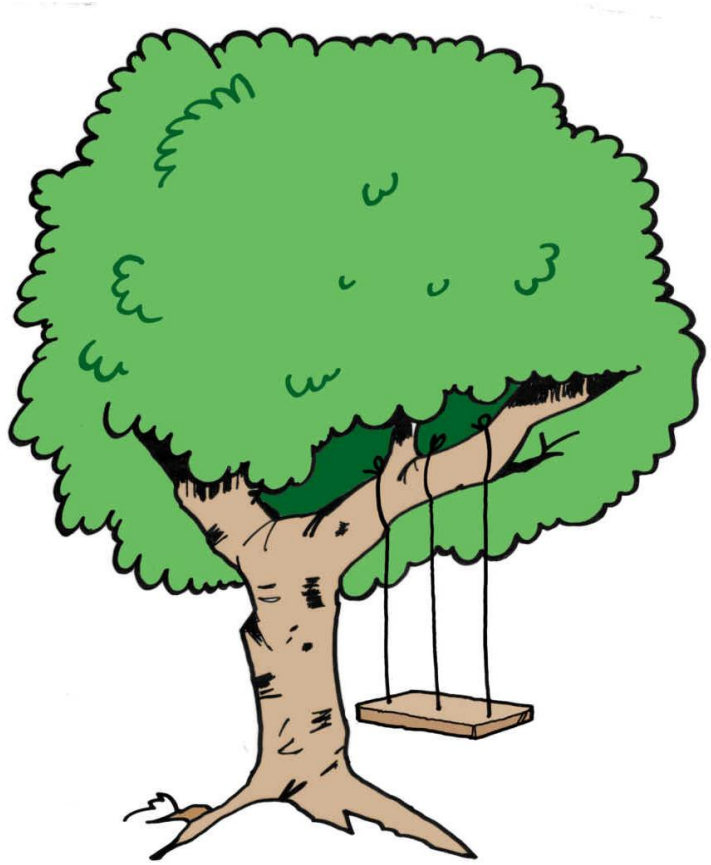
To, co opowiedział audytor:



Narzędzia wspomagające audytora

Jak rozmawiać z IT???

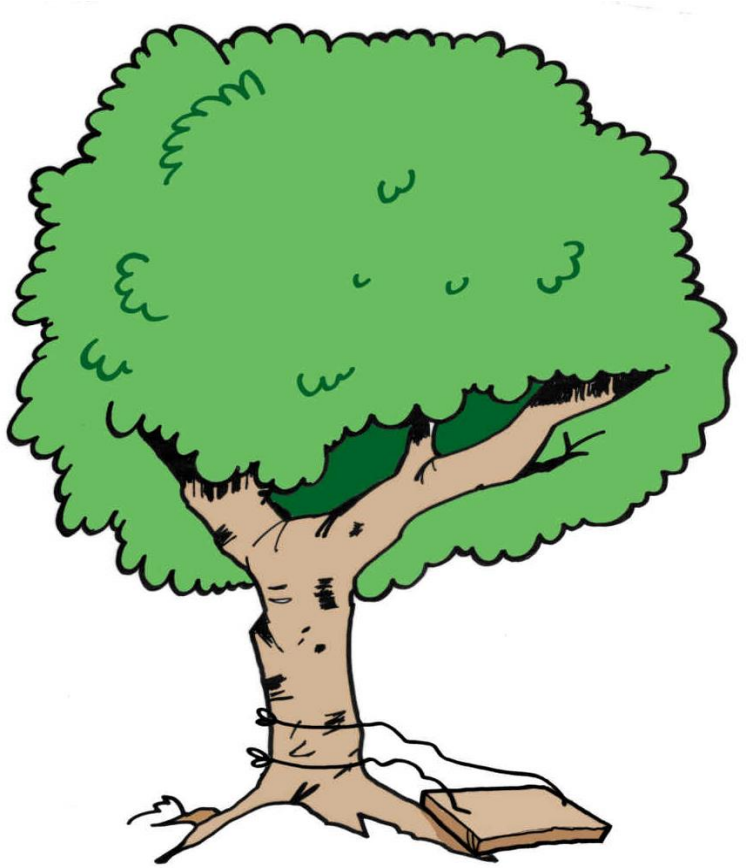
To, co zapisał w notatkach informatyk:



Narzędzia wspomagające audytora

Jak rozmawiać z IT???

To, jak rozumiał zadanie informatyk jak brał się do pracy:



Narzędzia wspomagające audytora

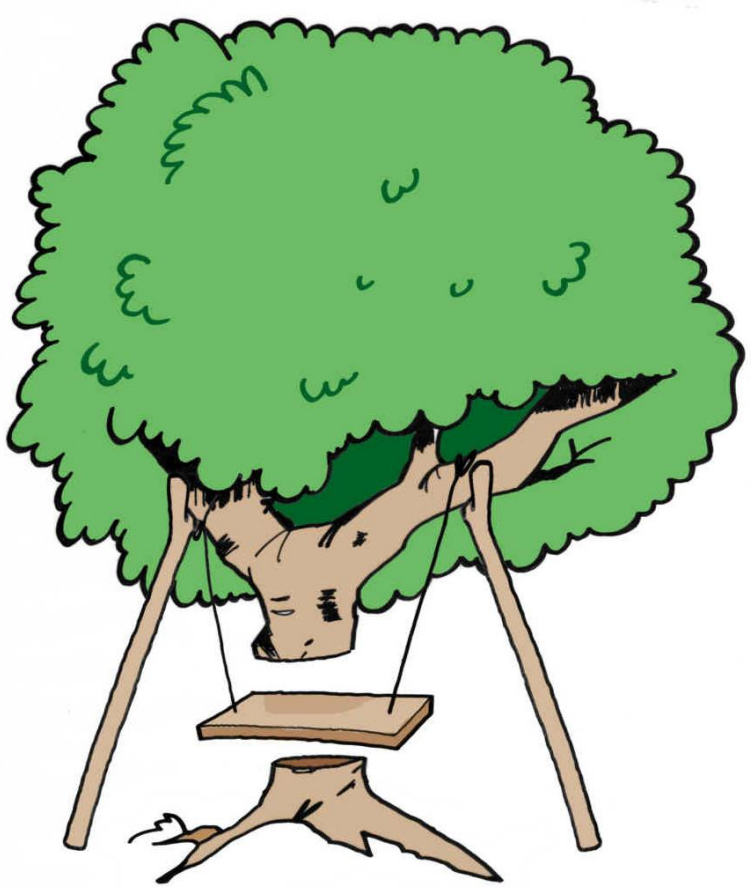
Jak rozmawiać z IT???

To, co wyprodukował informatyk:

Narzędzia wspomagające audytora

Jak rozmawiać z IT???

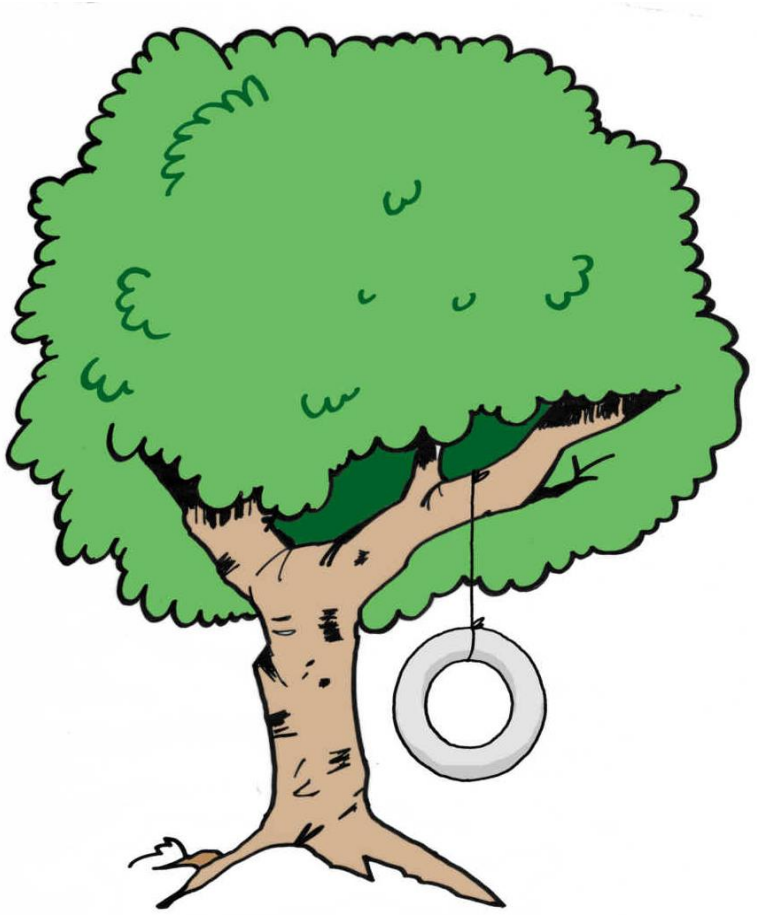
To, co informatyk przekazał audytorowi:



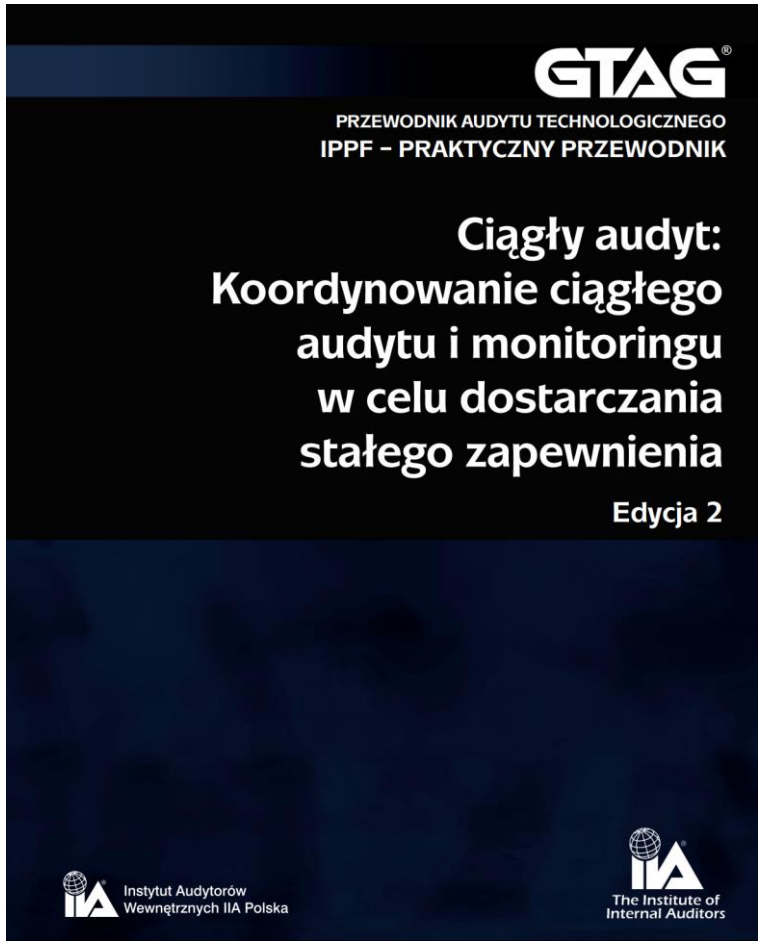
Narzędzia wspomagające audytora

Jak rozmawiać z IT???

To, czego faktycznie potrzebował audytor:



Audyt ciągły



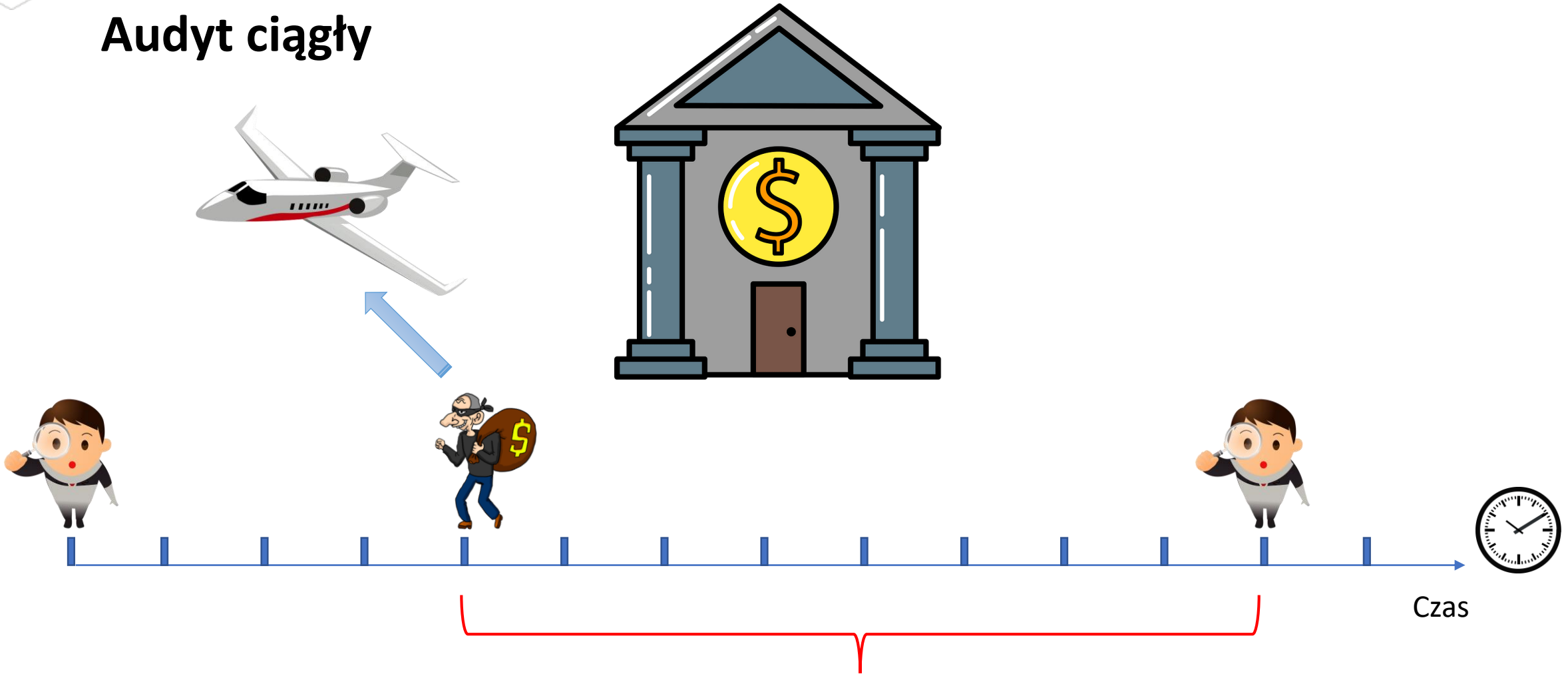
Ciągły audyt – kombinacja wspomaganej technologicznie bieżącej oceny ryzyka i kontroli. Ciągły audyt został zaprojektowany tak, by umożliwiać audytorom wewnętrznym raportowanie na zadany temat w znacznie krótszym czasie niż w przypadku tradycyjnego podejścia retrospektywnego.

Audyt ciągły

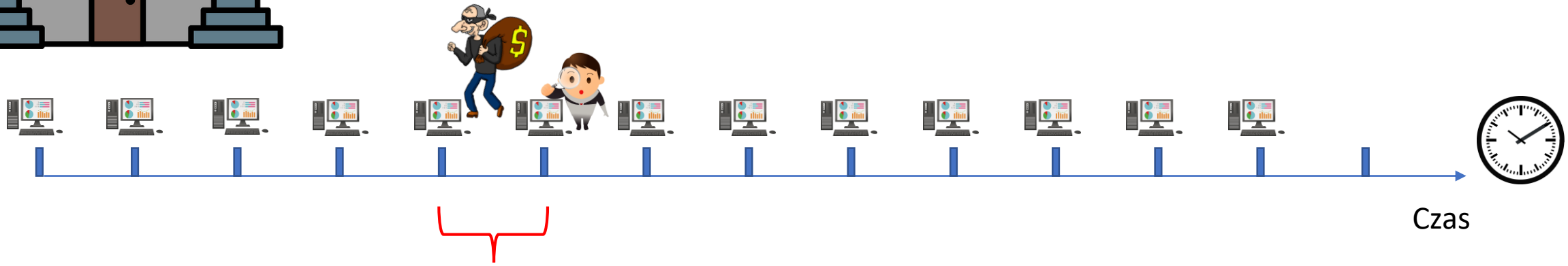
Etapy wdrażania:

1. Opracowanie strategii ciągłego audytu.
2. Uzyskiwanie danych do rutynowego wykorzystania.
3. Formułowanie wskaźników ciągłego audytu (bieżąca ocena ryzyka oraz bieżąca ocena kontroli).
4. Przekazywanie wyników i zarządzanie nimi.

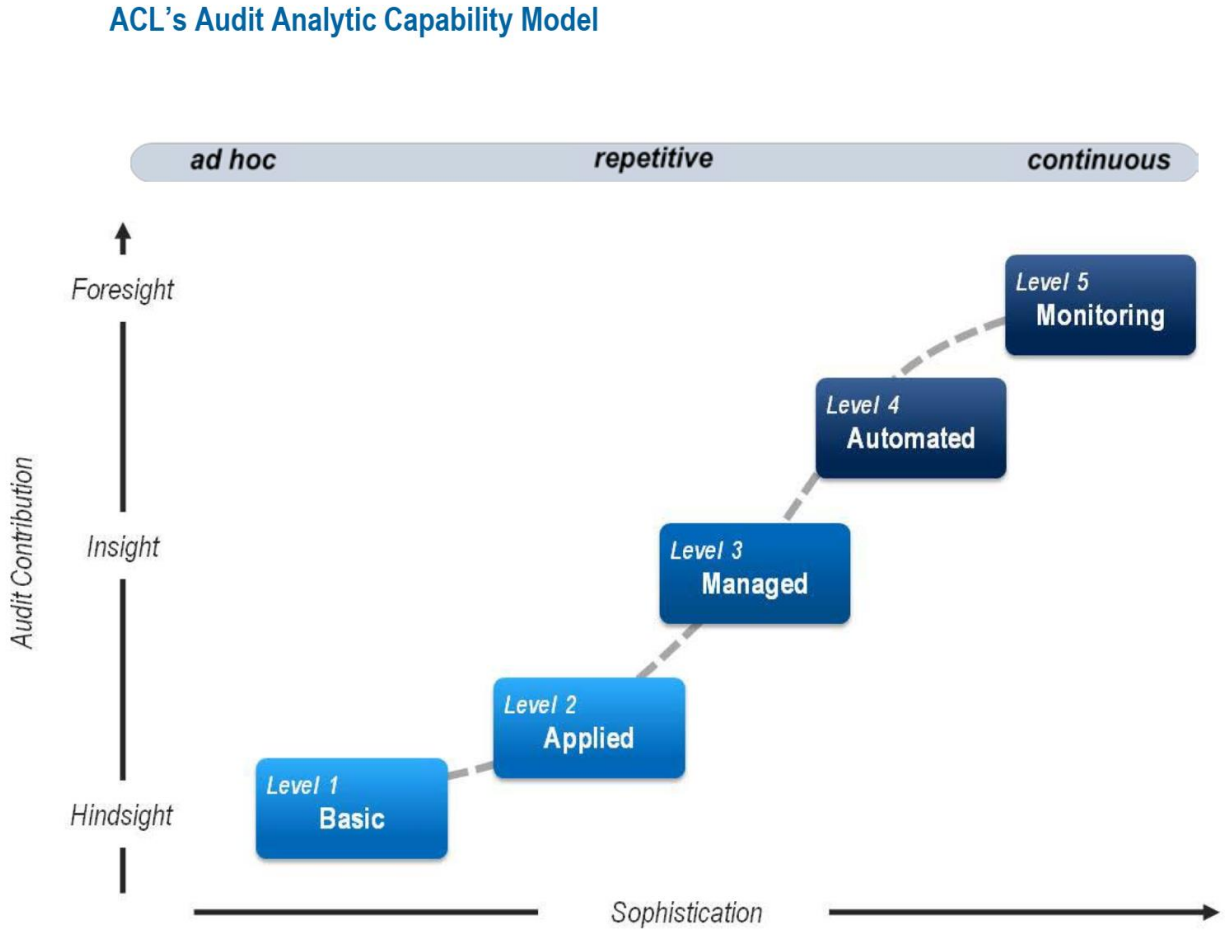
Audyt ciągły



Audyt ciągły



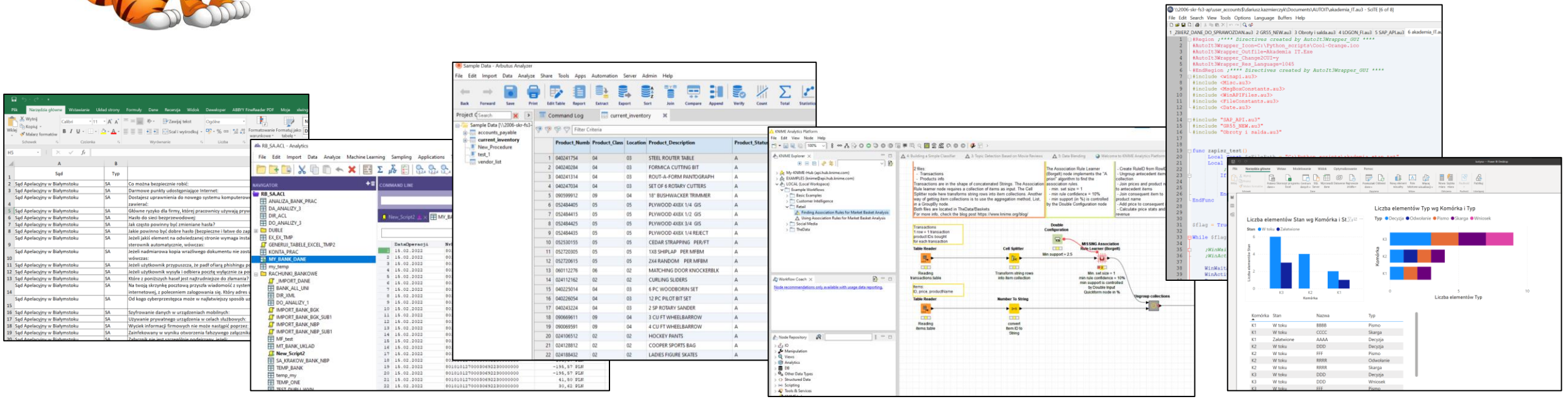
Audyt ciągły



A gdzie my jesteśmy???

Narzędzia wspomagające audytora i audyt ciągły – jak to działa?

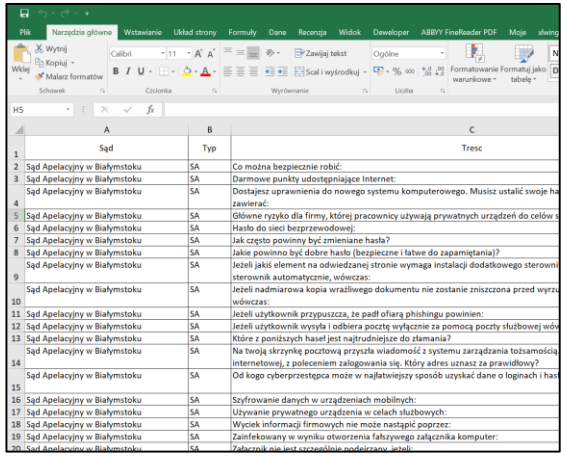
A teraz… to, co tygrysy lubią najbardziej. ☺



Narzędzia wspomagające audytora i audyt ciągły – jak to działa?

1. Pytanie szefa: Czy aby dobrze wypłacamy pracownikom wynagrodzenie?

MS Excel



	A	B	C
1	Sąd	Typ	Tresc
2	Sąd Apelacyjny w Białymstoku	SA	Co można bezpiecznie robić:
3	Sąd Apelacyjny w Białymstoku	SA	Darmowe punkty udostępniające Internet:
4	Sąd Apelacyjny w Białymstoku	SA	Dostajesz uprawnienia do nowego systemu komputerowego. Musisz ustalić swoje ha zawierać:
5	Sąd Apelacyjny w Białymstoku	SA	Główne ryzyko dla firmy, której pracownicy używają prywatnych urządzeń do celów s
6	Sąd Apelacyjny w Białymstoku	SA	Hasło do sieci bezprzewodowej:
7	Sąd Apelacyjny w Białymstoku	SA	Jak często powinny być zmieniane hasła?
8	Sąd Apelacyjny w Białymstoku	SA	Jakie powinno być dobre hasło (bezpieczne i łatwe do zapamiętania)?
9	Sąd Apelacyjny w Białymstoku	SA	Jeżeli jakiś element na odwiedzanej stronie wymaga instalacji dodatkowego sterowni sterownik automatycznie, wówczas:
10	Sąd Apelacyjny w Białymstoku	SA	Jeżeli nadmiarowa kopia wrażliwego dokumentu nie zostanie zniszczona przed wyrzu wówczas:
11	Sąd Apelacyjny w Białymstoku	SA	Jeżeli użytkownik przypuszcza, że padł ofiarą phishingu powinien:
12	Sąd Apelacyjny w Białymstoku	SA	Jeżeli użytkownik wysyła i odbiera pocztę wyłącznie za pomocą poczty służbowej wów
13	Sąd Apelacyjny w Białymstoku	SA	Które z poniższych haseł jest najtrudniejsze do złamania?
14	Sąd Apelacyjny w Białymstoku	SA	Na twoją skrzynkę pocztową przyszła wiadomość z systemu zarządzania tożsamością internetowej, z poleceniem zalogowania się. Który adres uznasz za prawidłowy?
15	Sąd Apelacyjny w Białymstoku	SA	Od kogo cyberprzestępca może w najłatwiejszy sposób uzyskać dane o loginach i has
16	Sąd Apelacyjny w Białymstoku	SA	Szyfrowanie danych w urządzeniach mobilnych:
17	Sąd Apelacyjny w Białymstoku	SA	Używanie prywatnego urządzenia w celach służbowych:
18	Sąd Apelacyjny w Białymstoku	SA	Wyciek informacji firmowych nie może nastąpić poprzez:
19	Sąd Apelacyjny w Białymstoku	SA	Zainfekowany w wyniku otworzenia fałszywego załącznika komputer:
20	Sąd Apelacyjny w Białymstoku	SA	Załącznik nie jest szczególnie podejrzany, jeżeli:

Co potrzeba?

1. ***Dane z systemu HR np. nr pracownika, nr rachunku bankowego, kwota angażu.***
2. ***Dane z systemu FK lub banku, gdzie są rejestrowane przelewy.***

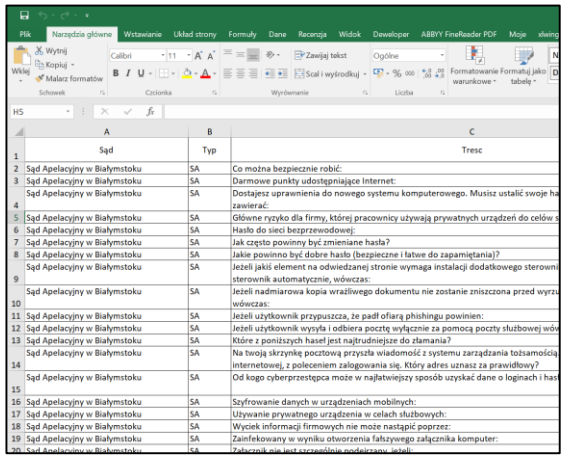
Czego szukamy?
Niezgodności lub potwierdzenia, że wszystko jest OK.

A jeśli musimy to weryfikować częściej???

Narzędzia wspomagające audytora i audyt ciągły – jak to działa?

2. Pytanie szefa: A może coś powie nam statystyka o naszych danych finansowych. Słyszałem coś o analizie Benforda.

MS Excel



	A	B	C
1	Sąd	Typ	Tresc
2	Sąd Apelacyjny w Białymstoku	SA	Co można bezpiecznie robić:
3	Sąd Apelacyjny w Białymstoku	SA	Darmowe punkty udostępniające Internet:
4	Sąd Apelacyjny w Białymstoku	SA	Dostajesz uprawnienia do nowego systemu komputerowego. Musisz ustalić swoje ha zawierać:
5	Sąd Apelacyjny w Białymstoku	SA	Główne ryzyko dla firmy, której pracownicy używają prywatnych urządzeń do celów s
6	Sąd Apelacyjny w Białymstoku	SA	Hasło do sieci bezprzewodowej:
7	Sąd Apelacyjny w Białymstoku	SA	Jak często powinny być zmieniane hasła?
8	Sąd Apelacyjny w Białymstoku	SA	Jakie powinno być dobre hasło (bezpieczne i łatwe do zapamiętania)?
9	Sąd Apelacyjny w Białymstoku	SA	Jeżeli jakiś element na odwiedzanej stronie wymaga instalacji dodatkowego sterowni sterownik automatycznie, wówczas:
10	Sąd Apelacyjny w Białymstoku	SA	Jeżeli nadmiarowa kopia wrażliwego dokumentu nie zostanie zniszczona przed wyrzu wówczas:
11	Sąd Apelacyjny w Białymstoku	SA	Jeżeli użytkownik przypuszcza, że padł ofiarą phishingu powinien:
12	Sąd Apelacyjny w Białymstoku	SA	Jeżeli użytkownik wysyła i odbiera pocztę wyłącznie za pomocą poczty służbowej wów
13	Sąd Apelacyjny w Białymstoku	SA	Które z poniższych haseł jest najtrudniejsze do złamania?
14	Sąd Apelacyjny w Białymstoku	SA	Na twoją skrzynkę pocztową przyszła wiadomość z systemu zarządzania tożsamością internetowej, z poleceniem zalogowania się. Który adres uznasz za prawidłowy?
15	Sąd Apelacyjny w Białymstoku	SA	Od kogo cyberprzestępca może w najłatwiejszy sposób uzyskać dane o loginach i hasł
16	Sąd Apelacyjny w Białymstoku	SA	Szyfrowanie danych w urządzeniach mobilnych:
17	Sąd Apelacyjny w Białymstoku	SA	Używanie prywatnego urządzenia w celach służbowych:
18	Sąd Apelacyjny w Białymstoku	SA	Wyciek informacji firmowych nie może nastąpić poprzez:
19	Sąd Apelacyjny w Białymstoku	SA	Zainfekowany w wyniku otworzenia fałszywego załącznika komputer:
20	Sąd Apelacyjny w Białymstoku	SA	Załącznik nie jest szczególnie podejrzany, jeżeli:

Co potrzeba?

Dane z systemu FK np. dziennika.

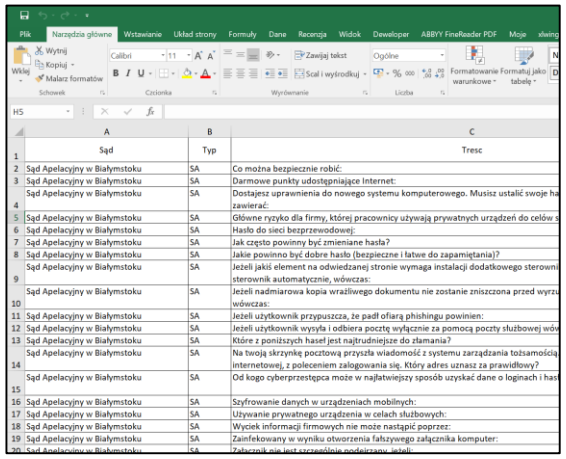
Czego szukamy?
Anomalii w rozkładzie Benforda.

A może coś warto automatyzować?

Narzędzia wspomagające audytora i audyt ciągły – jak to działa?

3. Pytanie szefa: Czy aby dobrze przekazujemy kwoty podatku VAT na właściwe konta kontrahentów? Ręczna weryfikacja może być nieskuteczna.

MS Excel + xlwing



	A	B	C
1	Sąd	Typ	Tresc
2	Sąd Apelacyjny w Białymstoku	SA	Co można bezpiecznie robić:
3	Sąd Apelacyjny w Białymstoku	SA	Darmowe punkty udostępniające Internet:
4	Sąd Apelacyjny w Białymstoku	SA	Dostajesz uprawnienia do nowego systemu komputerowego. Musisz ustalić swoje ha zawierać:
5	Sąd Apelacyjny w Białymstoku	SA	Główne ryzyko dla firmy, której pracownicy używają prywatnych urządzeń do celów s
6	Sąd Apelacyjny w Białymstoku	SA	Hasło do sieci bezprzewodowej:
7	Sąd Apelacyjny w Białymstoku	SA	Jak często powinny być zmieniane hasła?
8	Sąd Apelacyjny w Białymstoku	SA	Jakie powinno być dobre hasło (bezpieczne i łatwe do zapamiętania)?
9	Sąd Apelacyjny w Białymstoku	SA	Jeżeli jakiś element na odwiedzanej stronie wymaga instalacji dodatkowego sterowni sterownik automatycznie, wówczas:
10	Sąd Apelacyjny w Białymstoku	SA	Jeżeli nadmiarowa kopia wrażliwego dokumentu nie zostanie zniszczona przed wyrzu wówczas:
11	Sąd Apelacyjny w Białymstoku	SA	Jeżeli użytkownik przypuszcza, że padł ofiarą phishingu powinien:
12	Sąd Apelacyjny w Białymstoku	SA	Jeżeli użytkownik wysyła i odbiera pocztę wyłącznie za pomocą poczty służbowej wów
13	Sąd Apelacyjny w Białymstoku	SA	Które z poniższych haseł jest najtrudniejsze do złamania?
14	Sąd Apelacyjny w Białymstoku	SA	Na twoją skrzynkę pocztową przyszła wiadomość z systemu zarządzania tożsamością internetowej, z poleceniem zalogowania się. Który adres uznasz za prawidłowy?
15	Sąd Apelacyjny w Białymstoku	SA	Od kogo cyberprzestępca może w najłatwiejszy sposób uzyskać dane o loginach i hasł
16	Sąd Apelacyjny w Białymstoku	SA	Szyfrowanie danych w urządzeniach mobilnych:
17	Sąd Apelacyjny w Białymstoku	SA	Używanie prywatnego urządzenia w celach służbowych:
18	Sąd Apelacyjny w Białymstoku	SA	Wyciek informacji firmowych nie może nastąpić poprzez:
19	Sąd Apelacyjny w Białymstoku	SA	Zainfekowany w wyniku otworzenia fałszywego załącznika komputer:
20	Sąd Apelacyjny w Białymstoku	SA	Załącznik nie jest szczególnie podejrzany, jeżeli:

Co potrzeba?

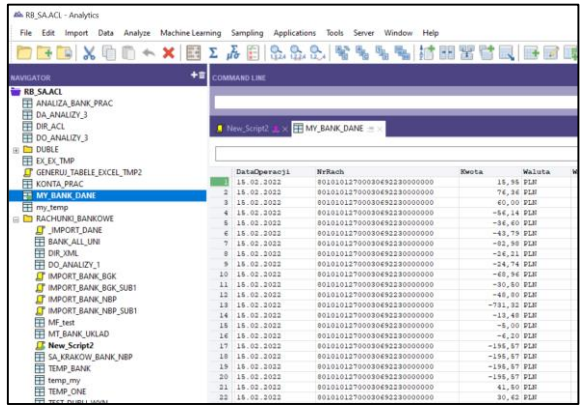
Dane z systemu FK lub banku, gdzie są podane rachunki bankowe kontrahentów.

A może warto usprawnić Excela?

Narzędzia wspomagające audytora i audyt ciągły – jak to działa?

4. Pytanie szefa: Czy jesteśmy bezpieczni w trybie pracy zdalnej? Jak się ma nasz VPN?

ACL/ Arbutus Analyzer



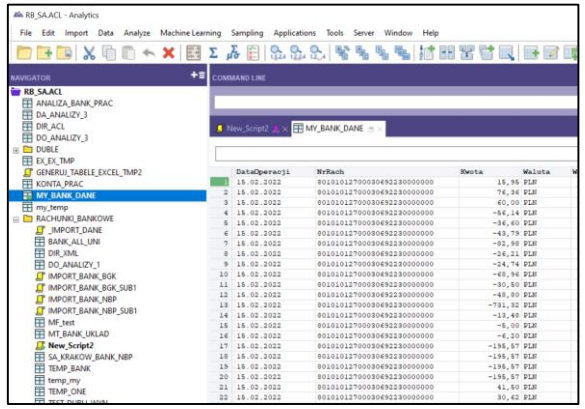
Co potrzeba?

Logi z urządzeń brzegowych sieci / serwery VPN etc.

Narzędzia wspomagające audytora i audyt ciągły – jak to działa?

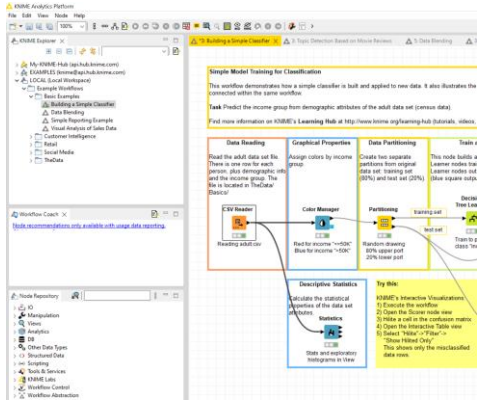
5. Pytanie szefa: Czy nasza księgowość dobrze się prowadzi? Jak nasza sprawozdawczość?

ACL/ Arbutus Analyzer/Knime



Co potrzeba?

Ewidencja księgowa, sprawozdawczość.

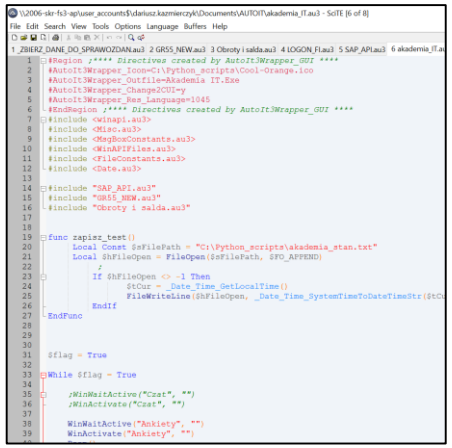


Narzędzia wspomagające audytora i audyt ciągły – jak to działa?

5. Pytanie szefa: Czy nasza księgowość dobrze się prowadzi? Jak nasza sprawozdawczość?

AutoIt / Python

Jak pobrać tyle danych???
Nie mamy przecież dostępu do bazy danych!!!



Narzędzia wspomagające audytora i audyt ciągły – jak to działa?

6. Pytanie szefa: Czy pracownicy czasem nie korzystają z maili służbowych do celów prywatnych?

Python

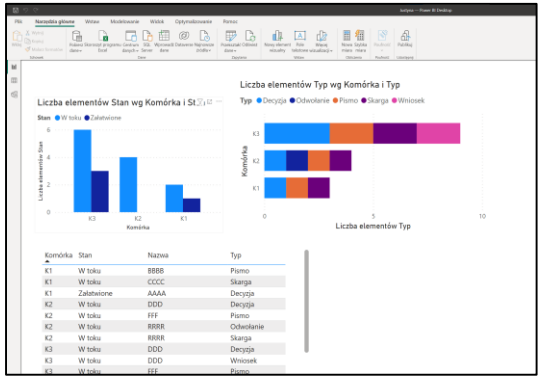
```
import time
import keyboard
import clipboard

time.sleep(5)

for osoba in dane_test:
    # if 'gov.pl' in osoba:
    pyautogui.click(4400, 860)
    pyautogui.hotkey('ctrl', 'a')
    keyboard.write(osoba)
    pyautogui.hotkey('enter')
    time.sleep(2.5)
    pyautogui.moveTo(3944, 1023)
    pyautogui.mouseDown()
    pyautogui.moveTo(6000, 1049)
    pyautogui.mouseUp()
    pyautogui.keyDown('ctrl')
    pyautogui.keyDown('c')
    pyautogui.keyUp('c')
```

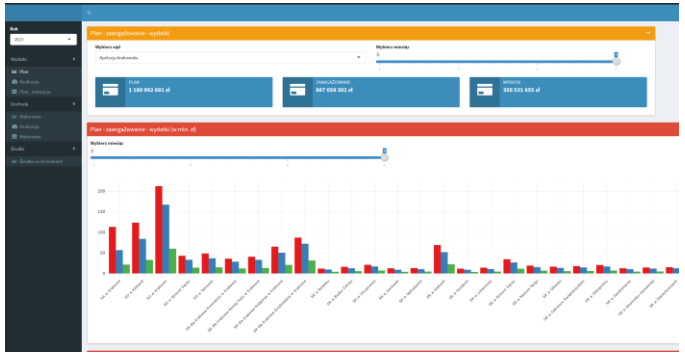
Jak odwoływać się do strony internetowej???
Jest API, ale płatne!!!

Narzędzia wspomagające audytora i audyt ciągły – jak to działa?

7. Pytanie szefa: Czy można te dane jakoś prezentować syntetycznie, nie w tabelkach? Tak na „rzut" okiem?

PowerBI/Python/R

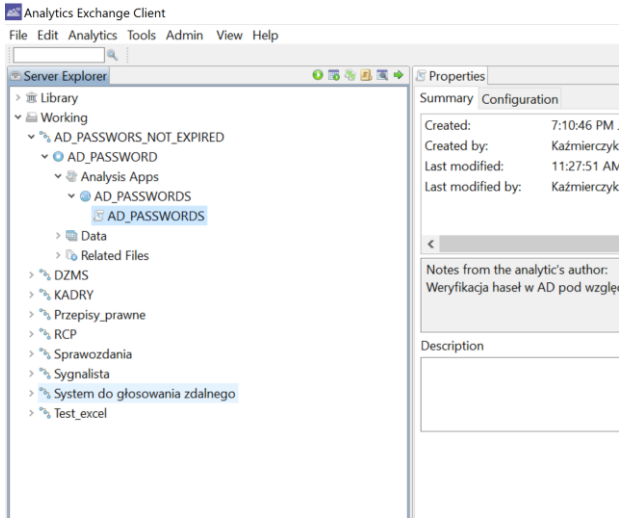




Narzędzia wspomagające audytora i audyt ciągły – jak to działa?

8. Pytanie szefa: Ok, ale czy pewne analizy mogą się wykonywać automatycznie?

Harmonogram Windows/AX Serwer/Python



Dziękuję za uwagę ☺

Dariusz Kaźmierczyk
kazmieda@poczta.fm
https://www.linkedin.com/in/dariusz-kazmierczyk-cgap-acda-6a985233