

## AUTOMATYZACJA - SYSTEM PRZEJMUJE WIELE PRACOCHŁONNYCH DZIAŁAŃ

Im więcej działań „przypilnuje i skoordynuje” system tym więcej czasu pozostaje na właściwą pracę.

**Audyt KSC** realizowany jest w oparciu o moduł Zarządzania Audytem Platformy BCMLogic. Wspierane są wszystkie jego etapy:

- Ustalenie zakresu
- Przypisanie zespołu audytorskiego
- Planowanie audytu
- Zbieranie i rejestrowanie informacji
- Identyfikacja nieprawidłowości oraz założeń
- Uzgodnienie raportu i akceptacja audytu
- Monitorowanie realizacji działań naprawczych

**Mechanizm Workflow** dba o automatyczne przekazywanie kontroli nad procesem do odpowiednich osób, wysyłając powiadomienie i nadając uprawnienia. W zależności od etapu procesu oraz roli, użytkownik widzi lub może edytować potrzebne w danym momencie zakładki. **Raport audytowy**, raz zdefiniowany w szablonie, jest automatycznie wypełniany danymi i nie ma potrzeby każdorazowego pisania go od początku. **Zalecenia audytowe** przypisywane są na poziomie audytu do poszczególnych osób, wraz z opisem zadania do wykonania oraz docelową datą. System wysyła powiadomienia o konieczności realizacji, zbliżającym się i przekroczonym terminie zakończenia. Oczywiście system może też wskazać na raporcie status rekomendacji w zależności od etapu wykonania, audytu, właściciela i wielu innych atrybutów.

Lista Usług Krytycznych	✓
Plan audytu i struktura zespołu	✓
Wsparcie przebiegu audytu	✓
Niezgodności i rekomendacje	✓
Uzgadnianie i akceptacja	✓
Raport i historia	✓

## LISTA USŁUG KRYTYCZNYCH

Opis	Nazwa	Pełnomocnik OUK	Koordynator	Jednostka organizacyjna	Status	Poziom
Prz	Przygotowanie raportu dla KNP	Naczelnik Joanna Jozwiak	Koordynator BCM	Departament IT	Aktywny	Poziom 2
Dok	Dokonanie rozliczeń transakcji krajowych	Dyrektor Kamila Haniłowska	Koordynator BCM	Departament Księgowości	Aktywny	Poziom 1

Dla każdej usługi gromadzone są potrzebne informacje.

**Parametry usługi:** Nazwa, lokalizacja, używane zasoby informatyczne, systemy informacyjne, opis kwalifikacji incydentu jako poważny.

**Osoby odpowiedzialne:** prezes/dyrektor generalny//CEO, Audytor wewnętrzny, Pełnomocnik, Nadzorujący audyt.

**Osoby odpowiedzialne za procesy zarządzania:** ryzykiem, incydentami, podatnościami, utrzymaniem, ciągłością działania itd.

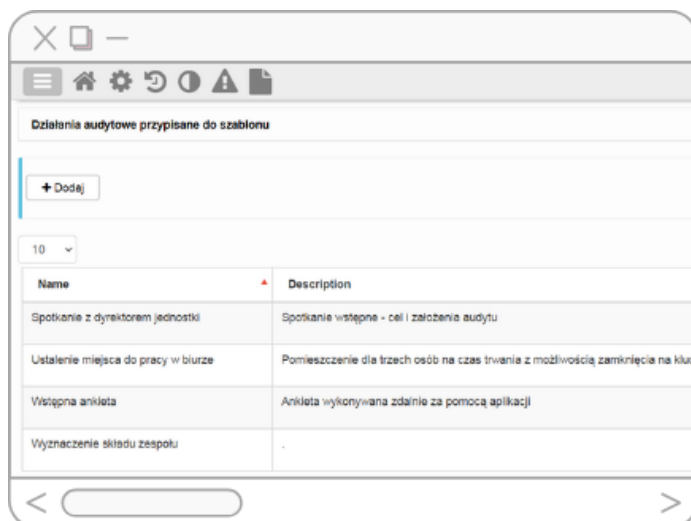
Te informacje używane przez aplikację w wielu miejscach. Przykładowo przy wskazywaniu osób odpowiedzialnych za poszczególne kategorie nieprawidłowości czy podczas akceptacji raportu. Zacztywanie danych z systemu zapewnia spójność oraz oszczędza czas ponieważ nie trzeba ich wprowadzać do dokumentu raportu.

## PLAN AUDYTU I STRUKTURA ZESPOŁU

**Biblioteka planów audytowych** – dla każdego audytu, w tym do KSC, można określić listę zadań korzystając z gotowych szablonów zdefiniowanych w Bibliotece. Szablon KSC obejmuje działania i obszary audytowe niezbędne dla tego typu.

**Rejestr działań audytowych** – utworzony na bazie biblioteki i/lub indywidualnie dodanych zadań. Stanowi listę kontrolną oraz może być automatycznie wstawiony do raportu audytowego. W trakcie jego trwania możliwa jest zmiana statusu, oznaczenie daty zmiany oraz dodanie komentarza. Typy zadań audytowych oraz statusów są parametryzowane w systemie do potrzeb organizacji (np. spotkanie, spotkanie zdalne, mail, telefon).

**Zespół audytowy** – wybór osób oraz przypisanie rodzaju pełnionej funkcji (audytor wiodący, systemów operacyjnych, zarządzania ISO itd.). Umożliwia to nadanie uprawnień i kontrolę dostępu, rejestrację, kto i kiedy wykonał zadanie, dodał spostrzeżenie i rekomendację oraz wysłanie powiadomienia czy udział w uzgodnieniu raportu.

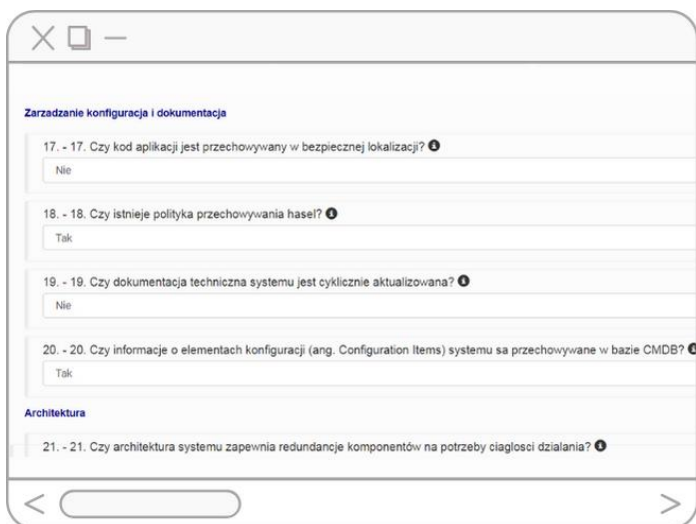


Name	Description
Spotkanie z dyrektorem jednostki	Spotkanie wstępne - cel i założenia audytu
Ustalenie miejsca do pracy w biurze	Pomieszczenie dla trzech osób na czas trwania z możliwością zamknięcia na klucz
Wstępna ankieta	Ankieta wykonywana zdalnie za pomocą aplikacji
Wyznaczenie składu zespołu	-

## WSPARCIE AUDYTU

**Ankiety audytowe** – aplikacja umożliwia zdefiniowanie i przypisanie do każdego z planowanych audytów jednej lub więcej dowolnych ankiet. Ankieta może być elementem pierwszego kontaktu z audytowaną jednostką – po jej wypełnieniu, informacja trafia zwrotnie do audytora i może posłużyć do dalszych działań. Ankiety mogą składać się z pytań podrzędnych, rozwijanych zależnie od wybranej odpowiedzi.

**Obszary** – rejestr czynności, ankiety oraz mechanizm rejestracji nieprawidłowości i rekomendacji pozwala przypisać aktywność do obszary. Domyślnie zdefiniowane są obszary dotyczące KSC: Organizacja zarządzania bezpieczeństwem informacji, Procesy zarządzania bezpieczeństwem informacji, Zarządzanie ryzykiem itd.



**Zarządzanie konfiguracją i dokumentacją**

17. - 17. Czy kod aplikacji jest przechowywany w bezpiecznej lokalizacji?  Nie

18. - 18. Czy istnieje polityka przechowywania haseł?  Tak

19. - 19. Czy dokumentacja techniczna systemu jest cyklicznie aktualizowana?  Nie

20. - 20. Czy informacje o elementach konfiguracji (ang. Configuration Items) systemu są przechowywane w bazie CMDB?  Tak

**Architektura**

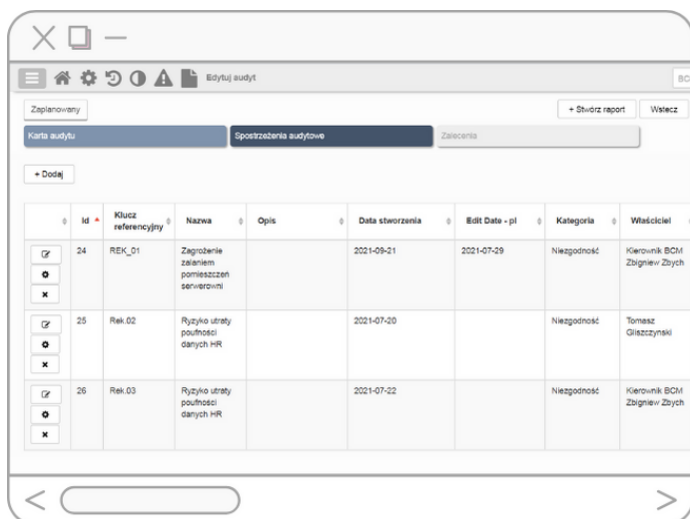
21. - 21. Czy architektura systemu zapewnia redundancję komponentów na potrzeby ciągłości działania?

## REJESTRACJA NIEPRAWIDŁOŚCI

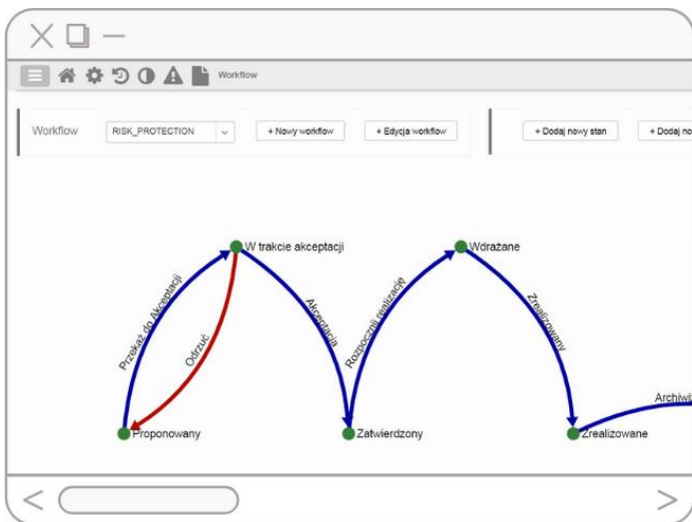
Każda nieprawidłowość jest przypisywana do obszaru (np. Bezpieczeństwo fizyczne) oraz nadany **poziom istotności**, na podstawie słownika: Krytyczny, Wysoki, Średni, Niski, Nie dotyczy). Raz wprowadzona nieprawidłowość jest automatycznie wstawiona do raportu generowanego na podstawie szablonu.

## ZARZĄDZANIE REKOMENDACJAMI

Do każdej nieprawidłowości można przypisać jedną lub więcej rekomendacji. Atrybuty rekomendacji to: nazwa, opis zadania, przypisana osoba i planowany termin zamknięcia, powiązana nieprawidłowość oraz klucz referencyjny.



ID	Klucz referencyjny	Nazwa	Opis	Data stworzenia	Edit Date - pl	Kategoria	Właściciel
24	REK_01	Zagrożenie zabaniem pomieszczeń serwerowni		2021-09-21	2021-07-29	Nie zgodność	Kierownik BCM Zbigniew Zych
25	Rek_02	Ryzyko utraty poufności danych HR		2021-07-20		Nie zgodność	Tomasz Głuszczynski
26	Rek_03	Ryzyko utraty poufności danych HR		2021-07-22		Nie zgodność	Kierownik BCM Zbigniew Zych



Kluczowymi elementami usprawniającym pracę z rekomendacji są:

**Workflow**, pozwalający na ustalenie statusów i możliwych przejść, automatyczne rejestrowanie przyjęcia rekomendacji oraz jej wykonania.

**Powiadomienia** dostarczane przez email, sms, system zgłoszeniowy lub dowolny system wystawiający odpowiednie API. Powiadomienia wynikają ze zmiany statusu *Workflow* lub tworzone są, jako przypomnienia – np. „zostało pięć dni do terminu wykonania działania”. Powiadomienia przypisane są do różnych zmian. W szablonach powiadomień określamy odbiorców (np. rola, grupa, właściciel i wiele innych), treść statyczną oraz dynamiczną, pobieraną z aplikacji w momencie generacji powiadomienia.

## UZGADNIANIE I AKCEPTACJA

Proces uzgodnienia odbywa się całkowicie w aplikacji. Odpowiednio zdefiniowany workflow pozwala audytorowi zmienić status i przekazać dostęp do dokumentu do osoby odpowiedzialnej za audytowane usługi. Przy czym aplikacja umożliwia kontrolę, które informacje są widoczne dla właściciel oraz czy może je edytować czy tylko odczytać. Zmieniając status, istnieje możliwość dodania własnego komentarza. Właściciel obszaru może zaakceptować wnioski lub zwrócić je do audytora z prośbą o uwzględnienie uwag. W każdym momencie uzgadniania, uprawnieni użytkownicy mogą wygenerować raport z audytu. Aplikacja przechowuje: datę zmiany statusu, użytkownika oraz przesłany komentarz

### Warto zapamiętać

- Wsparcie dla całego procesu Zarządzania Audytem
- Workflow* definiuje i automatyzuje pełny cykl życia audytu, pozwalając na różny sposób działania zależnie od typu audytu
- Schemat akceptacji* jest elementem określającym dodatkowy krok w *Workflow*, tam gdzie wymagane jest podjęcie i zarejestrowanie decyzji lub wyrażenie opinii
- W jednym miejscu w aplikacji oraz w raportach
- Precyzyjny mechanizm uprawnień dba o to, jakie ekrany i jaki zakres informacji użytkownik widzi lub edytuje
- Integracja z systemem kadrowym oraz zarządzającym uprawnieniami pozwala

Przebieg audytu, obserwacje oraz rekomendacje dostępne

### Jak wygląda wdrożenie?

- Warsztat, który pozwala dopasować konfigurację
- W ciągu 3-5 tygodni dajemy do dyspozycji moduł dopasowany do potrzeb
- Weryfikujemy działania i ergonomię działania z użytkownikami biznesowymi
- Szkolimy użytkowników
- Wspólnie przygotowujemy raporty i dashboardy
- Uruchomiony system