testerzy.pl

Usługa: Audyt kodu źródłowego

Audyt kodu źródłowego jest kompleksową usługą , której głównym celem jest weryfikacja jakości analizowanego kodu, jego skalowalności, łatwości utrzymania, poprawności i stabilności działania, jak również identyfikacja naruszeń bezpieczeństwa.

Pozwala także na wykrycie złożonych problemów pozostających w ukryciu, a których wystąpienie może mieć katastrofalne skutki dla samego systemu oraz danych w nim zawartych.

www.testerzy.pl
tel. 32 733 09 58
email: kontakt@testerzy.pl

Wynikiem audytu jest raport zawierający podsumowanie wniosków z przeprowadzonej analizy, znalezione błędy bądź uwagi wraz z oceną ryzyka z nimi związanego oraz rekomendacje odnośnie ewentualnych modyfikacji.

Audytowane technologie

Audyt może być wykonywany dla różnych typów aplikacji i technologii, w jakiej dany system został stworzony. Wykonujemy audyty systemów w technologiach:

- PHP
- Java
- C / C++ / C#
- Assembler
- MySQL
- HTML5, CSS3, JS, jQuery
- SOAP / REST
- inne.

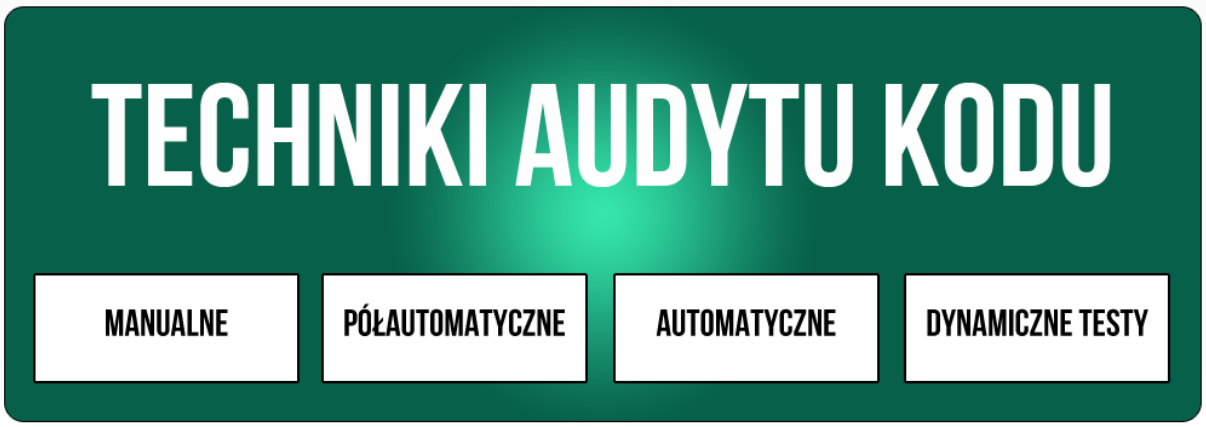
Zakres

Zakresem audytu kodu źródłowego objęta jest:

- analiza jakości kodu, w skład której wchodzi m.in. identyfikacja odstępstw od standardów, weryfikacja stosowania optymalnych praktyk wytwarzania oprogramowania, weryfikacja stosowania przyjętych reguł dotyczących czytelności kodu, implementacji przyjętych zasad formatowania oraz odpowiedniego dokumentowania kodu
- analiza łatwości utrzymania kodu źródłowego
- analiza kosztów wprowadzania zmian oraz stopnia odporności na modyfikacje
- analiza czytelności kodu oraz stopnia jego przyswajalności przez nowych członków zespołu
- analiza stabilności i poprawności działania
- analiza skalowalności kodu źródłowego
- analiza modularności i łatwości rozwoju kodu
- analiza zastosowanych technologii rozumiana jako zasadność i poprawność ich użycia, analiza kosztów ich utrzymania, kosztów rozwoju i kosztów wprowadzania zmian
- analiza przyjętej architektury systemu oraz poprawnego wykorzystania zastosowanego frameworka
- analiza odpowiedniego zastosowania wzorców projektowych
- analiza stopnia pokrycia testów jednostkowych i ich jakości
- analiza podatności na ataki typu XSS, Sql Injection, CSRF, DoS
- analiza optymalizacji i stopnia normalizacji bazy danych.

Stosowane techniki

W ramach realizacji usługi stosowane są następujące techniki:



- techniki manualne – manualny przegląd wybranych fragmentów kodu systemu, wykonywany przez audytorów
- techniki półautomatyczne – stosowane w celu wykrycia fragmentów kodu potencjalnie nadających się do bardziej szczegółowej analizy, wykorzystujące wybrane narzędzia oraz bazujące na doświadczeniu audytorów
- techniki automatyczne – statyczna oraz dynamiczna analiza kodu, wykonywana w oparciu o wiedzę i doświadczenie audytorów, przy użyciu wybranych narzędzi
- dynamiczne testy na uruchomionym i działającym systemie, których głównym celem jest znalezienie awarii, problemów związanych z walidacją oraz luk bezpieczeństwa.

Dla kogo pracujemy?

Naszą ofertę cechuje duża elastyczność względem Klienta. Współpracujemy z wytwórcami oprogramowania, wspierając zespoły projektowe, jak i z zamawiającymi oprogramowanie, wspomagając odbiór systemu w trakcie testów akceptacyjnych. Pracujemy z projektami wytwarzanymi w różnych modelach produkcji oprogramowania. Mamy doświadczenie zarówno w projektach wykorzystujących model kaskadowy, przyrostowy jak również techniki programowania zwinnego.

Wspieramy zespoły zarówno w początkowych etapach wytwarzania oprogramowania, identyfikując problemy jakości kodu już w jego wczesnym stadium rozwoju, jaki i w fazach końcowych. Oceniamy zdolność kodu do bycia rozwijanym, jego odporność na modyfikacje oraz szacujemy koszt wprowadzania zmian. Rekomendujemy wdrożenie kodu na produkcję oraz dokonujemy oceny stopnia możliwości i ryzyka dalszego utrzymania istniejącego systemu.

Pracujemy dla projektów ograniczonych czasowo, budżetowo bądź funkcjonalnie.

Proces

1. Cele
W tej fazie wspólnie z Klientem definiowane są cele audytu oraz określany jest zakres i czynności wymagane do osiągnięcia zakładanych celów. Aby osiągnąć zakładane cele wymagana jest współpraca Klienta oraz dostarczenie jak najpełniejszej dokumentacji systemu.

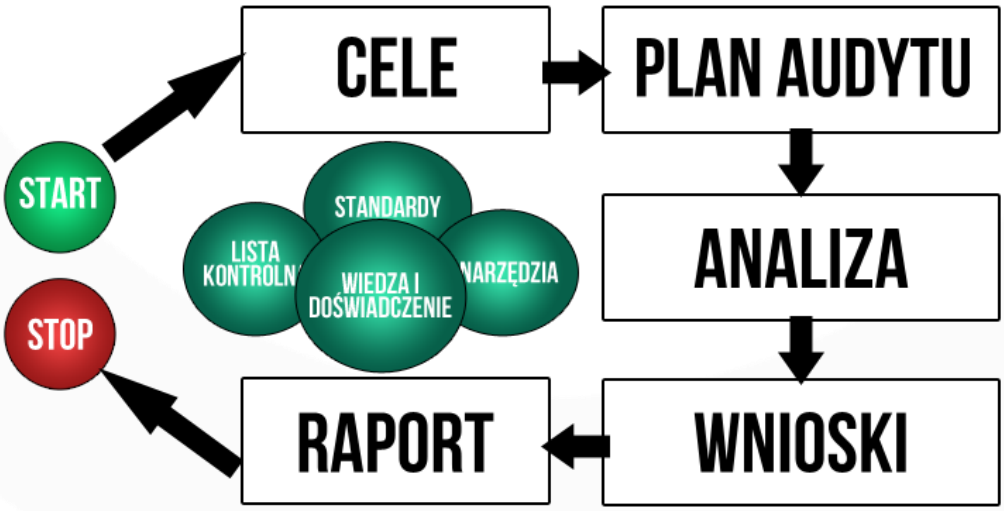
2. Plan audytu
Wstępnej analizie poddane zostają przesłane próbki kodu technologii mających podlegać audytowi. Analizowane są wszystkie uzyskane od Klienta informacje jak opis architektury systemu, wykorzystane technologie, liczba linii kodu dla poszczególnych technologii, dokumentacja techniczna, dokumentacja użytkownika czy sprecyzowane wymagania.

Na bazie wstępnej analizy tworzony jest plan audytu, wybierane są narzędzia, które zostaną użyte w trakcie analizy, wspólnie z Klientem ustalona zostaje metoda audytu (zgodność z określonymi standardami, własna lista kontrolna) oraz poziom szczegółowości oceny.

3. Analiza
Wykonanie analizy odbywa się według wcześniej ustalonego planu i wybranej metody, z użyciem wybranych narzędzi, w przewidzianym i ustalonym czasie. Wykonywane są wszystkie czynności wymagane do osiągnięcia zdefiniowanych celów pod kątem wybranego zakresu.

4. Wnioski
Rejestrowane są wszystkie wnioski oraz uwagi z przeprowadzonej analizy.

5. Raport i zakończenie audytu
Dostarczona zostaje niezależna ocena systemu w postaci szczegółowego raportu na bazie wniosków z przeprowadzonej analizy oraz wspólnie z Klientem analizowane są kryteria zakończenia audytu.



www.testerzy.pl
tel. 32 733 09 58
email: kontakt@testerzy.pl

Czas trwania

Czas trwania projektu jest szacowany indywidualnie uwzględniając zdefiniowane cele oraz zakres prac i czynności niezbędne do realizacji założonych celów. W oparciu o wstępne rozpoznanie systemu na bazie przesłanych próbek kodu wybranych technologii mających podlegać audytowi oraz wszystkich informacji o systemie dostarczonych przez Klienta, nasi specjaliści dokonują wstępnych szacunków pracochłonności wykonania projektu.

Dostawa klienta

W celu osiągnięcia założonych celów wymagana jest współpraca Klienta na każdym etapie realizacji projektu oraz dostarczenie jak najpełniejszej dokumentacji systemu. Wszelkie informacje jak opis architektury systemu, wykorzystane technologie, liczba linii kodu dla poszczególnych technologii, dokumentacja techniczna, dokumentacja użytkownika czy sprecyzowane wymagania, pomogą dokładniej oszacować koszty i czas wykonania usługi, a także dadzą naszym ekspertom dodatkową wiedzę, która będzie miała przełożenie na wykonanie samej analizy.

Uzyskując dostęp do działającego systemu, czy to poprzez dostarczenie działającej aplikacji wraz z poprawną konfiguracją i niezbędnym środowiskiem bądź dostając dostęp do systemu pracującego wyłącznie w sieci wewnętrznej, eksperci będą mieli możliwość zastosowania niektórych technik audytu, które nie mogłyby zostać użyte nie posiadając takiego dostępu.

Koszty

Koszty wykonania usługi szacowane są indywidualnie w oparciu o wstępne rozpoznanie systemu oraz na bazie określonych celów, zdefiniowanego zakresu prac i czynności warunkujących realizację celów. Dokonując wstępnej analizy przesłanych przez Klienta próbek kodu wybranych technologii mających podlegać audytowi oraz wszystkich uzyskanych od Klienta informacji o systemie, wykonujemy wstępne szacunki kosztowności wykonania usługi.

Korzyści dla klienta

Audyty kodu źródłowego w naszej firmie prowadzone są przez najlepszych ekspertów w branży. Dysponują oni doświadczeniem i praktyką zarówno w wielkich, jak i mniejszych projektach informatycznych na przestrzeni wielu lat.

Spośród wielu korzyści płynących z przeprowadzenia audytu kodu źródłowego, do najważniejszych należą:

- identyfikacja błędów programowych i odstępstw od standardów
- wykrycie problemów związanych z optymalizacją zaimplementowanych rozwiązań
- wykrycie podatności i luk, które do tej pory nie zostały zidentyfikowane

- weryfikacja stabilności i skalowalności kodu, jego czytelności, modularności oraz stopnia jego przyswajalności i łatwości uczenia się
- ocena łatwości utrzymania kodu, odporności na modyfikacje oraz szacunek kosztów wprowadzania zmian
- weryfikacja stopnia pokrycia testów jednostkowych i ich jakości
- identyfikacja podatności i ryzyka

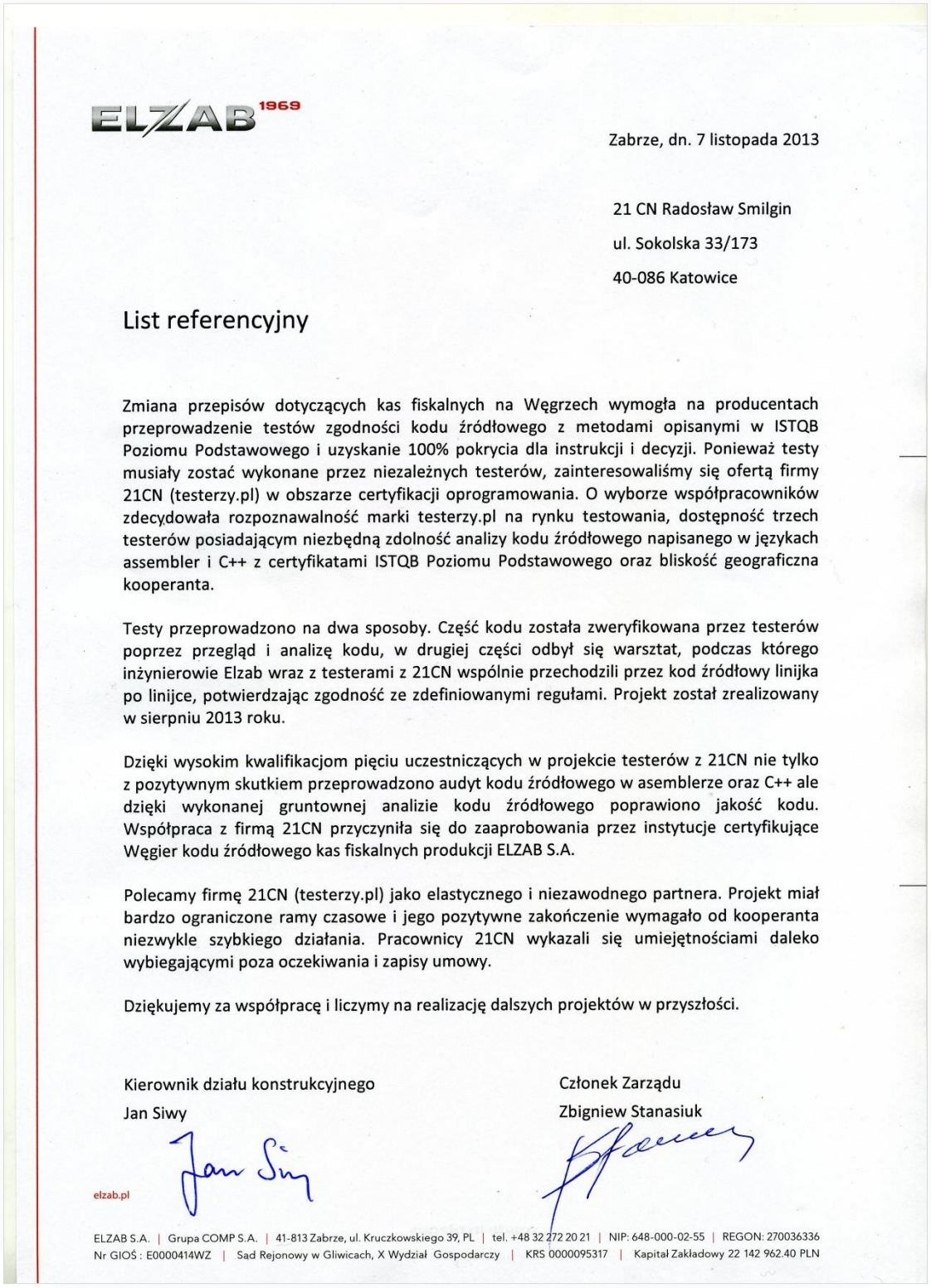
Naszą ofertę cechuje elastyczność względem Klienta oraz elastyczny model rozliczeń, gdzie płacą Państwo jedynie za realnie przepracowane godziny.

Wartość dodana

W ostatniej fazie audytu uzyskają Państwo niezależną ocenę audytowanego systemu, dostarczoną w postaci raportu. W zależności od zdefiniowanego zakresu audytu i wyznaczonych celów, raport zawierać będzie informacje na temat wniosków płynących z przeprowadzonej analizy, ocenę jakości kodu systemu, a także informacje o podatnościach, uwagach, zagrożeniach i ryzyku z nimi związanego. Dodatkowo mogą Państwo uzyskać certyfikat potwierdzający jakość dostarczanego systemu, jako wynik certyfikacji oprogramowania dostarczanej przez testerzy.pl (http://testerzy.pl/certyfikacja-oprogramowania)

testerzy.pl

Referencje



ELZAB 1969

Zabrze, dn. 7 listopada 2013

21 CN Radosław Smilgin
ul. Sokolska 33/173
40-086 Katowice

List referencyjny

Zmiana przepisów dotyczących kas fiskalnych na Węgrzech wymogła na producentach przeprowadzenie testów zgodności kodu źródłowego z metodami opisanymi w ISTQB Poziomu Podstawowego i uzyskanie 100% pokrycia dla instrukcji i decyzji. Ponieważ testy musiały zostać wykonane przez niezależnych testerów, zainteresowaliśmy się ofertą firmy 21CN (testerzy.pl) w obszarze certyfikacji oprogramowania. O wyborze współpracowników zdecydowała rozpoznawalność marki testerzy.pl na rynku testowania, dostępność trzech testerów posiadającym niezbędną zdolność analizy kodu źródłowego napisanego w językach assembler i C++ z certyfikatami ISTQB Poziomu Podstawowego oraz bliskość geograficzna kooperanta.

Testy przeprowadzono na dwa sposoby. Część kodu została zweryfikowana przez testerów poprzez przegląd i analizę kodu, w drugiej części odbył się warsztat, podczas którego inżynierowie Elzab wraz z testerami z 21CN wspólnie przechodzili przez kod źródłowy linijka po linijce, potwierdzając zgodność ze zdefiniowanymi regułami. Projekt został zrealizowany w sierpniu 2013 roku.

Dzięki wysokim kwalifikacjom pięciu uczestniczących w projekcie testerów z 21CN nie tylko z pozytywnym skutkiem przeprowadzono audyt kodu źródłowego w asemblerze oraz C++ ale dzięki wykonanej gruntownej analizie kodu źródłowego poprawiono jakość kodu. Współpraca z firmą 21CN przyczyniła się do zaaprobowania przez instytucje certyfikujące Węgier kodu źródłowego kas fiskalnych produkcji ELZAB S.A.

Polecamy firmę 21CN (testerzy.pl) jako elastycznego i niezawodnego partnera. Projekt miał bardzo ograniczone ramy czasowe i jego pozytywne zakończenie wymagało od kooperanta niezwykle szybkiego działania. Pracownicy 21CN wykazali się umiejętnościami daleko wybiegającymi poza oczekiwania i zapisy umowy.

Dziękujemy za współpracę i liczymy na realizację dalszych projektów w przyszłości.

Kierownik działu konstrukcyjnego
Jan Siwy

Członek Zarządu
Zbigniew Stanasiuk

elzab.pl

ELZAB S.A. | Grupa COMP S.A. | 41-813 Zabrze, ul. Kruczkowskiego 39, PL | tel. +48 32 272 20 21 | NIP: 648-000-02-55 | REGON: 270036336
Nr GIOŚ : E0000414WZ | Sad Rejonowy w Gliwicach, X Wydział Gospodarczy | KRS 0000095317 | Kapitał Zakładowy 22 142 962.40 PLN

URZĄD MARSZAŁKOWSKI
WOJEWÓDZTWA MAŁOPOLSKIEGO

Kraków, dnia 29 marca 2016 r.

Nasz znak: OR-VII.272.4.2015

List referencyjny

Niniejszym potwierdzam, że firma 21CN Radosław Smilgin z siedzibą przy ul. Sokolskiej 33/173, 40-086 Katowice w grudniu 2015 r. na zlecenie Urzędu Marszałkowskiego Województwa Małopolskiego przeprowadziła audyt kodu źródłowego systemu informatycznego. Prace obejmowały przygotowanie i przeprowadzenie audytu kodu źródłowego wraz ze wszystkimi narzędziami deweloperskimi (środowiskiem deweloperskim) oraz przygotowanie raportu z audytu.

W ramach architektury systemu poddanego audytowi można wyróżnić kilka modułów, w tym elektroniczny obieg dokumentów oraz moduł kadrowo – płacowy. System zbudowany jest w oparciu o Oracle Application Development Framework (ADF) i język Java.

Wykonane przez firmę 21CN Radosław Smilgin usługi zostały zrealizowane profesjonalnie, z należytą starannością, zgodnie z zawartą umową i w wyznaczonym terminie.

Wynagrodzenie za ww. prace wyniosło [redacted] zł brutto.

Niniejsze referencje wydaje się na prośbę zainteresowanego.

Zastępca Dyrektora
Departamentu Organizacyjno-Prawnego
Andrzej Masny

ul. Basztowa 22
31-156 Kraków
adres do korespondencji: ul. Racławicka 56, 30-017 Kraków