Załącznik nr 2

OPIS FUNKCJONALNOŚCI SYSTEMU DO ZARZĄDZANIA RYZYKIEM (RM)

1.1. Zgodność z normami ISO 31000:2018, ISO 27005:2018, ISO 27001:2017 oraz ISO 22301:2020, a także ISO 27799:2016 i ISO 27002:2017.

1.2. Zgodność z RODO - Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

1.3. Zgodność z obowiązującą Ustawą o krajowym systemie cyberbezpieczeństwa wraz z rozporządzeniami szczególnie w kontekście zakresu obowiązków Operatora Usługi Kluczowej.

1.4. Zgodność z wymaganiami audytu oceny Operatora Usługi Kluczowej zgodnie z Krajowym Systemem Cyberbezpieczeństwa w zakresie zgodności z Ustawą o krajowym systemie cyberbezpieczeństwa (Ustawa z dnia 05 lipca 2018 Dz.U. 2018 poz. 15601), szczególnie (ale nie tylko) w zakresie zarzadzania ryzykiem (Obszar 3) – zgodnie z szablonem opublikowanym przez Ministerstwo Cyfryzacji 28 kwietnia 2020 r. – Załącznik nr 12.

1.5. Art. 226 Ustawy z dnia 26.04.1974 r. Kodeks pracy (Dz.U. Nr 21, poz. 94 z późn. zm.) - Pracodawca ocenia i dokumentuje ryzyko zawodowe związane z wykonywaną praca oraz stosuje niezbędne środki profilaktyczne zmniejszające ryzyko, informuje pracowników o ryzyku zawodowym, które wiąże się z wykonywaną pracą, oraz o zasadach ochrony przed zagrożeniami.

2.1. System do zarządzania ryzykiem uwzględnia podział ról w procesie zarządzania ryzykiem wraz z możliwością konfiguracji i dostosowania do potrzeb wynikających z danego obszaru. System umożliwia również powiązanie kont użytkowników z domeną Active Directory poprzez zarządzanie uprawnieniami na podstawie RBAC – (Role-Based Access Control).

2.2. System do zarządzania ryzykiem umożliwia sprawne zarządzanie dużą liczbą ryzyk (najmniej jeden tysiąc), z podziałem na obszary działania, role, dopasowane do struktury organizacyjnej Centrum-e-zdrowia, procesy i komórki organizacyjne oraz samodzielne stanowiska pracy.

2.3. System do zarządzania ryzykiem:

2.3.1. umożliwia implementację i wspomaga metodykę zarządzania ryzykiem w celu zapewnienia zgodności z wymaganiami audytu w zakresie zarządzania ryzykiem Operatora Usługi Kluczowej zgodnie z Krajowym Systemem Cyberbezpieczeństwa w zakresie zgodności z Ustawą o krajowym systemie cyberbezpieczeństwa, szczególnie – zgodnie z szablonem opublikowanym przez Ministerstwo Cyfryzacji 28 kwietnia 2020 r[2], w tym również zapewniać symultaniczną obsługę procesów zarządzania ryzykiem adekwatną dla zakresów poszczególnych Usług Kluczowych w organizacji.

2.3.2. umożliwia tworzenie i definiowanie metodyk zarządzania ryzykiem (w oparciu o różne wzory i mechanizmy) dostosowanych do obszarów i poszczególnych

[1] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560
[2] https://mc.bip.gov.pl/krajowy-system-cyberbezpieczenstwa/operatorzy-uslug-kluczowych/szablon-sprawozdania-z-audytu-zgodnego-z-ustawa-o-krajowym-systemie-cyberbezpieczenstwa.html

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

kontekstów i atrybutów, w tym m.in. atrybutów bezpieczeństwa informacji, jak poufność, integralność, dostępność, autentyczność, oraz zabezpieczeń, krytyczności. W szczególności system umożliwia dowolne agregowanie podstawowych aktywów organizacji wprowadzonych do systemu, stosowanie wobec w/w agregacji innych metodyk zarządzania ryzykiem w celu odwzorowania specyficznych procesów biznesowych.

2.3.3. umożliwia realizację analizy ryzyka w bezpieczeństwie informacji zgodną z ISO 31000:2018, ISO 27005:2018 w powiązaniu z ISO 27001:2017 – w zakresie możliwości mitygacji ryzyk, stosownie do mechanizmów zabezpieczających.

2.3.4. umożliwia uwzględnienie zastosowania kontekstu organizacyjnego dla każdego ze zdefiniowanych i konfigurowalnych obszarów (maksymalna wymagana ilość obszarów to 50). Kluczowym jest obszar Departamentu Bezpieczeństwa w tym cyberbezpieczeństwa, bezpieczeństwa informacji, obejmujący wszystkie wymagane obszary wskazane w Załączniku nr 2 do OPZ.

2.3.5. umożliwia prowadzenie rejestru ryzyk, wraz z możliwością śledzenia i przeglądu historii ryzyk – w tym historię każdego ryzyka z osobna, zarówno w procesie przeglądu jak i szacowania, analizy ryzyka,

2.3.6. umożliwia komunikację pomiędzy uczestnikami zaangażowanymi w proces zarządzania ryzykiem, polegającą na wysyłaniu powiadomień do osób odpowiedzialnych w procesie zarządzania ryzykiem o pojawiających się zadaniach do realizacji czy wprowadzonych analizach, szacowaniach gotowych do akceptacji,

2.3.7. umożliwia wyznaczanie poziomu tolerancji ryzyka, oraz umożliwia definiowanie i wybór planów oraz sposobów postępowania z ryzykiem w odniesieniu do wyznaczonej tolerancji, poprzez posiadanie funkcjonalności, w której będzie można definiować takie plany, przypisywać osoby odpowiedzialne, rejestrować zadania, śledzić postępy, wysyłać powiadomienia,

2.3.8. umożliwia szacowanie i ocenę ryzyk z analizą skuteczności mechanizmów kontrolnych,

2.3.9. umożliwia przeprowadzenie procesu szacowania ryzyka w kontekście zasadności instalacji systemów: przeciwpożarowego, systemu podtrzymania i stabilizacji energii elektrycznej, zabezpieczeń alarmowego i antynapadowego, instalacji systemu zabezpieczeń (drzwi / okna / ściany), podtrzymania warunków temperatury, wilgotności i wentylacji pomieszczeń.

2.3.10. ma możliwość tworzenia diagramów procesów BPMN[3] o stopniu szczegółowości biznesowej,

2.3.11. ma dołączone diagramy BPMN z wdrożonych w nim procesów zarządzania ryzykiem, oraz zapewnia ich edycję wraz z rozwojem i dostosowywaniem metodyki do potrzeb.

2.3.12. umożliwia prowadzenie kart ryzyk,

2.3.13. w ramach konfiguracji Systemu do zarządzania ryzykiem i dostosowywania umożliwia tworzenie i wiązanie formularzy wraz z relacjami,

2.3.14. umożliwia wizualizację ryzyk i analiz w postaci konfigurowalnych dashboardów

[3] Business Process Model and Notation, BPMN (Notacja i Model Procesu biznesowego) – graficzna notacja służąca do opisywania procesów biznesowych. – (źródło: https://pl.wikipedia.org/wiki/Business_Process_Modeling_Notation”

z prezentowaniem na nich danych w formie tabelarycznej, wykresów czy opisów,

2.3.15. umożliwia automatyczne powiadomienia, monity mailowe (m.in. przypomnienia o nadchodzących terminach, nowych ryzykach, incydentach, zdarzeniach, przekroczeniach poziomów ryzyk poza zdefiniowany poziom).

2.3.16. umożliwia konfigurowalne, automatyczne wysyłane raporty (oraz na żądanie) – w definiowalnych interwałach czasowych,

2.3.17. umożliwia generowanie raportów z analizy ryzyk do formatów minimalnie: .XLSX, .PDF, oraz do dashboardów w wersji graficznej.

2.3.18. umożliwia import danych do bibliotek, definicji, formularzy minimalnie z plików płaskich .txt, oraz posiadać instrukcję i procedurę w języku polskim - jak realizować krok po kroku.

2.3.19. umożliwia import danych konfiguracyjnych w formie minimalnie płaskich tabel w plikach tekstowych.

2.3.20. umożliwia szacowanie wartości ryzyk, z predefiniowanymi, konfigurowalnymi słownikami i szablonami, metodami i wzorami potrzebnych do notacji.

2.3.21. umożliwia okresowe automatyczne generowanie predefiniowanych raportów w tym w formie graficznej, tabelarycznej, opisowej, również np. w formie prezentacji macierzy i map ryzyka.

2.3.22. umożliwia ocenę krytyczności procesów, zagrożeń ciągłości działania zgodnie z ISO 22301:2020.

2.3.23. umożliwia opracowywanie i przygotowywanie raportów indywidualnych, poprzez m.in. filtrowanie danych ze względu na konfigurowalne kryteria i zdefiniowane kwerendy i zapytania.

2.3.24. umożliwia definiowanie, tworzenie i zapisywanie formularzy, skryptów i monitów wg konfigurowalnych parametrów.

2.3.25. umożliwia wprowadzanie i monitorowanie zdarzeń operacyjnych, incydentów w związku z bieżącą działalnością, oraz na tej podstawie m.in. umożliwiać wprowadzania planów działania,

2.3.26. umożliwia dokonanie szacowania ryzyk powiązanych ze zdarzeniami, incydentami, również w oparciu o zgormadzone dane historyczne,

2.3.27. instrukcja obsługi powinna być poza dostarczoną w pliku/plikach PDF oraz zaszyta w system w formie „dymków" lub podpowiedzi.

2.3.28. działa w środowisku Windows Server 2016,

2.3.29. ma włączoną funkcję szyfrowania TLS 1.2, z udostępnionym przez Zamawiającego certyfikatem.

2.3.30. Silnik bazy danych Systemu jest oparty o aktualną i wspieraną wersję przez producenta MS SQL 2016.

2.3.31. umożliwia śledzenie, audyt zmian w konfiguracji oprogramowania i bazy danych. Baza danych ma zaimplementowaną i włączoną funkcję audytu bazy danych, polegającą na rejestrowaniu działań wszystkich użytkowników.

2.3.32. po stronie klienta jest obsługiwany poprzez znane przeglądarki wiodących producentów i jest aktualizowany, aby w czasie trwania umowy zapewnić ciągłość działania poprzez m.in. wsparcie i obsługę (m.in. Edge, FireFox, Chrome).

2.3.33. posiada kreator umożliwiający dodawanie i konfigurowanie, parametrów,

formularzy i ankiet w systemie nie wymagający wiedzy programistycznej.

2.3.34. umożliwia sprawną pracę dla najmniej 80 osób jednocześnie, z możliwością w przypadku nieobecności danego pracownika zastąpienia go innym.

2.3.35. jest wyposażony przez producenta w API, umożliwiające jego przyszłą integrację z systemami zewnętrznymi i posiadać do niego czytelną dokumentację techniczną, umożliwiającą jego wykorzystanie przez developerów, m.in. do np. zasilania podatnościami, incydentami, czy danymi z innych systemów bezpieczeństwa jak SIEM[4], DLP[5], EDR[6], skaner podatności, antywirus, firewall[7], itp., oraz ticketowych - Jira / Jira Service Desk.

2.3.36. ma możliwość eksportu danych, raportów z analiz do formatu Microsoft Excela oraz formatu PDF.

2.3.37. posiada możliwość rozwijania samodzielnie przez Zamawiającego rozwiązania m.in. przez dodawanie kolejnych obszarów zarządzania ryzykiem.

3.1. strategiczny i zarządzania,

3.2. zarządzania portfelem projektów,

3.3. ochrona danych osobowych - ODO,

3.4. bezpieczeństwo w tym bezpieczeństwo informacji,

3.5. obszar P1,

3.6. obszar EWP,

3.7. obszar SMZ,

3.8. eksploatacja i rozwój systemów informatycznych,

3.9. obsługa prawna,

3.10. finanse i księgowość,

3.11. kontrola zarządcza,

3.12. rozwoju Systemu e-Zdrowie,

3.13. BHP,

3.14. zakupy i zamówienia publiczne,

3.15. komunikacja,

3.16. wsparcia organizacji,

3.17. centrum analiz,

3.18. zarządzanie ryzykiem,

3.19. wdrożeń Systemu e-Zdrowia,

3.20. audyt wewnętrzny,

3.21. architektura i usługi e-zdrowia,

3.22. interoperacyjność.

[4] SIEM - to skrót od Security Information and Event Management
[5] DLP - Data Loss Prevention
[6] EDR (Endpoint Detection and Response)
[7] firewall - rodzaj zapory sieciowej