POLSKIE TOWARZYSTWO INFORMATYCZNE

Izba Rzeczoznawców

Ekspertyza

zawierająca ocenę skutków dla bezpieczeństwa informacji

projektu z dnia 22 listopada 2019 r.
Rozporządzenia Ministra Finansów
w sprawie kas rejestrujących mających postać oprogramowania

przygotowanego na podstawie art. 111b ust. 3 pkt 1 i 2 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2018 r. poz. 2174, z późn. zm.)

Paweł Henig – kierownik Zespołu wykonawców

Ekspertyza została wykonana na podstawie umowy zawartej w dniu 10 grudnia 2019 r. pomiędzy COMP S.A. a Polskim Towarzystwem Informatycznym.

Warszawa, 13 grudnia 2019 roku

Spis treści

Spis Rysunków

1. Wstęp

Niniejsza ekspertyza została opracowana przez Zespół Rzeczoznawców pod kierunkiem Pawła Heniga rzeczoznawcy Polskiego Towarzystwa Informatycznego na podstawie umowy z dnia 10 grudnia 2019 roku zawartej pomiędzy Polskim Towarzystwem Informatycznym a COMP S.A. z siedzibą w Warszawie, przy ul. Jutrzenki 116, kod pocztowy 02-230, zwanym w dalszej części opracowania **Zamawiającym** lub w skrócie **COMP**.

Sformułowano ją w oparciu o niżej wymienione materiały udostępnione przez Zamawiającego.

1. Projekt z dnia 22 listopada 2019 r. Rozporządzenia Ministra Finansów w sprawie kas rejestrujących mających postać oprogramowania przygotowany na podstawie art. 111b ust. 3 pkt 1 i 2 ustawy z dnia 11 mar-ca 2004 r. o podatku od towarów i usług (Dz. U. z 2018 r. poz. 2174, z późn. zm.) – zwany w dalszej części ekspertyzy **Projektem**.
2. Ocena skutków regulacji – dokument 4279101.
3. Uzasadnienie – dokument 427911.
4. Załącznik nr 1 do **Projektu** „Wymagania techniczne dla kas" – dokument 427915.
5. Załącznik nr 2 do **Projektu** „Logo fiskalne" – dokument 427914.
6. Załącznik nr 3 do **Projektu** „Wzór informacji o zasadach ewidencji" – dokument 427913.
7. Załącznik nr 4 do **Projektu** „Wzór wniosku o wyrejestrowanie kasy z ewidencji kas" – dokument 427912.

W opinii uwzględniono informacje zawarte w niżej wymienionych dokumentach, wybranych przez rzeczoznawcę do realizacji niniejszej ekspertyzy.

1. Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas –Standardy kryptograficzne. Wersja 2.0.0 z dnia 25 czerwca 2018r. (BIP MF).
2. Opis techniczny protokołu komunikacyjnego kasa – Centralne Repozytorium Kas –Specyfikacja komend. Wersja 1.0.0 z dnia 25 czerwca 2018r. (BIP MF).
3. Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j Dz. U. z 2018 r. poz. 2174, z późn. zm.).
4. Rozporządzenie Ministra Przedsiębiorczości i Technologii z dnia 28 maja 2018 r. w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące (Dz.U. z 2018 r. poz. 1206).
5. Rozporządzenie Ministra Finansów z dnia 29kwietnia 2019r.w sprawie kas rejestrujących (Dz.U. z 2019 r. poz. 816).
6. Ustawa z dnia 29 sierpnia 1997r. Ordynacja podatkowa (t.j. Dz. U. z 2019 r. poz. 900 z późn. zm.).
7. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych

1 Nr dokumentu nadawany w systemie Rządowego Centrum Legislacji:
https://legislacja.rcl.gov.pl/projekt/12323808/katalog/12623102

i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwane dalej **RODO**.

8. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560) zwana dalej **KSC**.
9. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247) zwane dalej **KRI**.
10. Norma PN-EN ISO/IEC 27001:2017-06 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji – Wymagania.
11. Norma PN-EN ISO/IEC 27002:2017-06 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji.

W trakcie realizacji ekspertyzy nie wystąpiła potrzeba kontaktu z Zamawiającym w celu udzielania dodatkowych wyjaśnień lub uzupełniania przekazanych materiałów.

2. Cel ekspertyzy

Celem ekspertyzy jest przeprowadzenie oceny skutków dla bezpieczeństwa informacji projektu z dnia 22 listopada 2019 r. Rozporządzenia Ministra Finansów w sprawie kas rejestrujących mających postać oprogramowania przygotowanego na podstawie art. 111b ust. 3 pkt 1 i 2 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2018 r. poz. 2174, z późn. zm.).

3. Opis przyjętych założeń i metody badania

Kasy rejestrujące stanowią jeden z elementów systemu informacyjnego Państwa w zakresie nadzoru nad podatnikami dokonującymi sprzedaży na rzecz osób fizycznych nieprowadzących działalności gospodarczej oraz rolników ryczałtowych, którzy są obowiązani prowadzić ewidencję sprzedaży przy zastosowaniu kas rejestrujących. Rejestracja czynności sprzedaży (z wykorzystaniem kas rejestrujących) jest podstawą rozliczenia należnego na rzecz skarbu państwa podatku. Oznacza to, że od jakości tej informacji zależy wysokość oraz termin zapłaty należnego podatku. Jakość informacji należy rozumieć jako autentyczność (niezaprzeczalność), dokładność oraz terminowość informacji wprowadzanych do systemu informacyjnego Państwa za pośrednictwem kas rejestrujących. Tym samym kasy rejestrujące stanowią nierozerwalny element tego systemu.

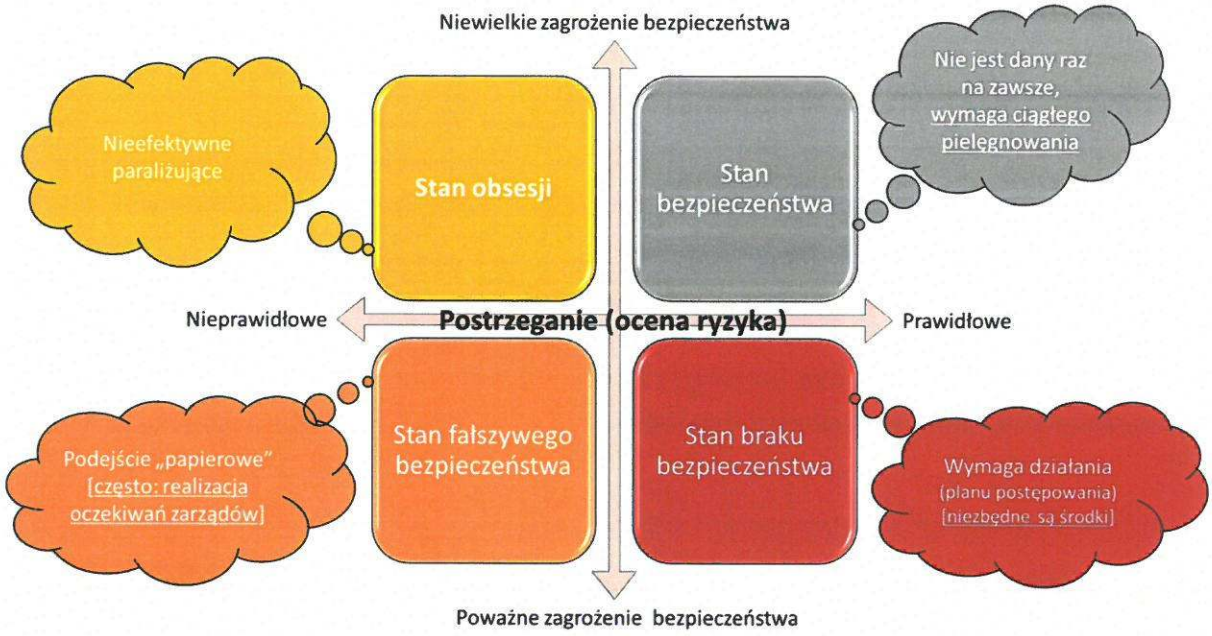
W ewidencji sprzedaży wykazuje się dane o sprzedaży, zawarte w dokumentach wystawianych przy zastosowaniu kas rejestrujących, w tym określające przedmiot opodatkowania, wysokość podstawy opodatkowania i podatku należnego oraz dane służące identyfikacji poszczególnych sprzedaży, w tym numer, za pomocą którego podatnik jest zidentyfikowany na potrzeby podatku albo podatku od wartości dodanej. Innymi słowy, jakość prowadzonej ewidencji sprzedaży przy zastosowaniu kas rejestrujących ma bezpośredni związek ze skutecznością poboru należnych podatków. Przekłada się to bezpośrednio na wymagania bezpieczeństwa informacji w tym systemie, gdyż utrata któregokolwiek atrybutu bezpieczeństwa informacji (takiego jak poufność, integralność, dostępność) w tym systemie zmaterializuje się w postaci strat budżetu państwa w formie niepobranych należnych podatków. Oznacza to, że prowadząc Ocenę Skutków Regulacji w tym przypadku należałoby oprzeć się również na obowiązujących przepisach w zakresie bezpieczeństwa informacji dla budowanego niniejszą regulacją systemu informacyjnego Państwa w zakresie nadzoru nad podatnikami. Zastosowanie w tym przypadku mają w szczególności:

- Rozporządzenie 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
- ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560);
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U 2017 poz. 2247).

Wspólną cechą wszystkich powyższych regulacji jest zarządzanie bezpieczeństwem oparte na ryzyku.

Bezpieczeństwo należy rozumieć w dwóch podstawowych aspektach: procesu i stanu. Bezpieczeństwo jako proces oznacza ciągłą działalność podmiotu (człowieka, społeczności lokalnych, narodów, państw itp.) w tworzeniu pożądanego stanu bezpieczeństwa. Stan bezpieczeństwa występuje wtedy, gdy zagrożenie zewnętrzne jest nieznaczne, a jego postrzeganie jest prawidłowe. Miarą postrzegania bezpieczeństwa jest ryzyko. Zależnie od metodyki oraz sposobu przeprowadzenia oceny ryzyka, jego postrzeganie może być prawidłowe lub nie. Nie

wykonując żadnej metodycznej analizy ryzyka, tak jak w przypadku udostępnionej Oceny Skutków Regulacji, nasze postrzeganie bezpieczeństwa z dużą dozą prawdopodobieństwa będzie nieprawidłowe. Brak metodycznej oceny ryzyka posiada jeszcze jedną wadę - nie daje się powtórzyć. To znaczy, że nie będzie można w stanie nadążać za zmianami w otoczeniu, w tym odpowiednio wcześnie nie zostaną zidentyfikowane podatności, których pojawienie się będzie miało konkretne implikacje w przyszłości. Związek pomiędzy postrzeganiem bezpieczeństwa (oceną ryzyka) a możliwością osiągnięcia stanu bezpieczeństwa przedstawia poniższy rysunek (opracowanie własne).



Rysunek 1 Stan bezpieczeństwa i jego postrzeganie.
Źródło: opracowanie własne.

Najbardziej pożądany stan bezpieczeństwa występuje wtedy, gdy występuje niewielkie zagrożenie dla bezpieczeństwa, które jest prawidłowo postrzegane. Stan bezpieczeństwa nie jest stanem stabilnym. Na skutek zmian w otoczeniu mogą pojawić się nowe zagrożenia dla bezpieczeństwa. Mogą być one skutkiem pojawienia się nowych podatności lub osłabieniem skuteczności wdrożonych zabezpieczeń. W tym przypadku, regularnie powtarzana ocena ryzyka powinna zidentyfikować stan braku bezpieczeństwa, a odpowiedni plan postępowania powinien pozwolić ponownie osiągnąć stan bezpieczeństwa. Oznacza to, że nawet stan braku bezpieczeństwa jest stanem korzystnym, ale tylko wtedy, gdy jest powiązany z realnym, czyli mającym pokrycie w odpowiednich zasobach, w tym środkach finansowych, planem działań.

Niewłaściwe postrzeganie stanu bezpieczeństwa jest zawsze niekorzystne. Jeżeli występuje w przypadku niewielkiego zagrożenia bezpieczeństwa (stan obsesji) to będzie powodowało nadmierne obciążenia utrudniające działanie, a tym samym będzie to stan, w którym będą ponoszone nadmierne koszty. Natomiast stan fałszywego bezpieczeństwa jest najbardziej niekorzystny, gdyż:

- z jednej strony usypiają czujność i dodatkowo osłabiają bezpieczeństwo,

- a z drugiej strony kumulują powstawanie długu w obszarze zabezpieczeń poprzez utrwalanie złych lub nieskutecznych nawyków (zachowań) lub rozwiązań technicznych.

Dokonanie systematycznej oceny ryzyka w zakresie bezpieczeństwa informacji i ciągłości działania wynika w tym przypadku nie tylko z obowiązujących przepisów prawa (**RODO**, **KSC** i **KRI**) lecz również z najlepszych praktyk zawartych w normach międzynarodowych. W szczególności istotne znaczenie mają wymienione wprost w przepisach prawa (lecz nie tylko) normy PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, PN-EN ISO 22301 oraz PN-ISO/IEC 29134.

Na potrzeby niniejszego opracowania wykorzystano w szczególności normy PN-EN ISO/IEC 27001 (załącznik normatywny A) oraz PN-EN ISO/IEC 27002 jako zbiór najlepszych praktyk w zakresie doboru zabezpieczeń w bezpieczeństwie informacji. Metodyka oceny ryzyka na potrzeby niniejszej ekspertyzy zostanie wykonana w trzech następujących krokach:

1) opracowanie modelu kasy rejestrującej zgodnie z obowiązującymi przepisami (**sprzętowa**);
2) opracowanie modelu kasy rejestrującej zgodnie z **Projektem** (**programowa**);
3) wykonanie porównawczej analizy ryzyka dla obu modeli z wykorzystaniem załącznika normatywnego A do normy PN-EN ISO/IEC 27001.

Prowadząc ocenę stopnia spełnienia wymagania zastosowano do oceny kryteria SPICE zgodnie z tabelą umieszczoną poniżej.

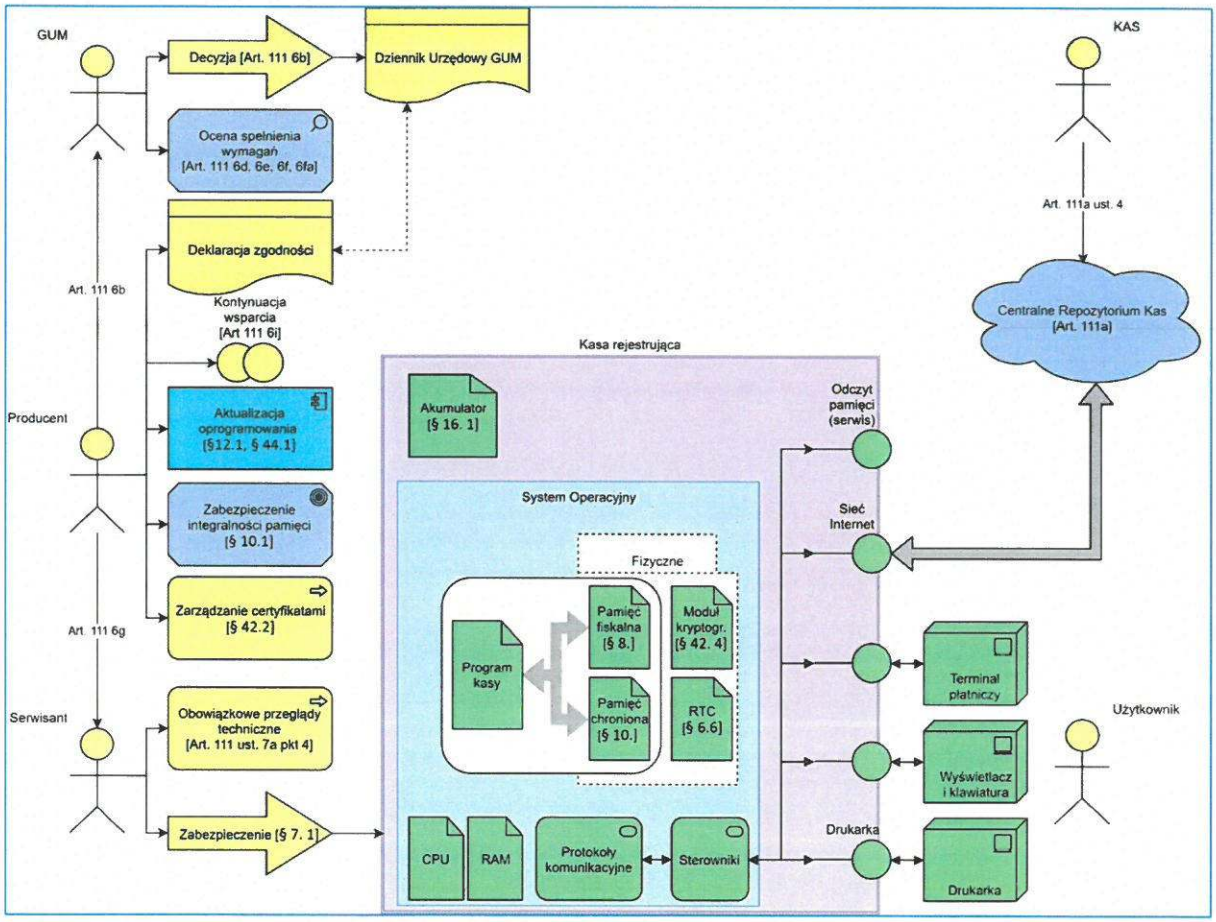
Oznaczenie	Znaczenie	% realizacji	Wyjaśnienie
N	Nie osiągnięto.	0–15%	Na tym poziomie nie istnieją dowody systematycznego osiągnięcia zdefiniowanego atrybutu w ocenianym procesie lub ich liczba jest znikoma.
P	Częściowo osiągnięto.	> 15–50%	Istnieją pewne dowody podejścia do (i częściowego osiągnięcia) zdefiniowanego atrybutu w ocenianym procesie. Niektóre aspekty osiągnięcia atrybutu mogą być niemożliwe do przewidzenia.
L	W znacznym stopniu osiągnięto.	> 50–85%	Istnieją dowody systematycznego podejścia do (i znacznego osiągnięcia) zdefiniowanego atrybutu w ocenianym procesie. W ocenianym procesie mogą istnieć pewne słabości związane z tym atrybutem.
F	W pełni osiągnięto.	> 85–100%	Istnieją dowody kompletnego i systematycznego podejścia do (i pełnego osiągnięcia) zdefiniowanego atrybutu w ocenianym procesie. W ocenianym procesie nie stwierdzono istotnych słabości związanych z tym atrybutem.
X	Nie dotyczy	nie dotyczy	Wymaganie nie ma zastosowania

4. Przebieg badania

4.1. Model kasy rejestrującej (sprzętowy)

Na podstawie wymagań dotyczących kas rejestrujących opracowano poniższy model. Poszczególne obiekty posiadają bezpośrednie odniesienie do wymagań zawartych w:

- ustawie z dnia 11 marca 2004 r. o podatku od towarów i usług odnosi się do artykułów (oznaczone na rysunku jako **Art.** z odniesieniem do właściwego numeru artykułu wraz z numerem ustępu po kropce)
- rozporządzeniu Ministra Przedsiębiorczości i Technologii z dnia 28 maja 2018 r. w sprawie kryteriów i warunków technicznych, którym muszą odpowiadać kasy rejestrujące odnosi się do paragrafów (oznaczone na rysunku jako **§** z odniesieniem do właściwego numeru paragrafu wraz z numerem punktu po kropce).

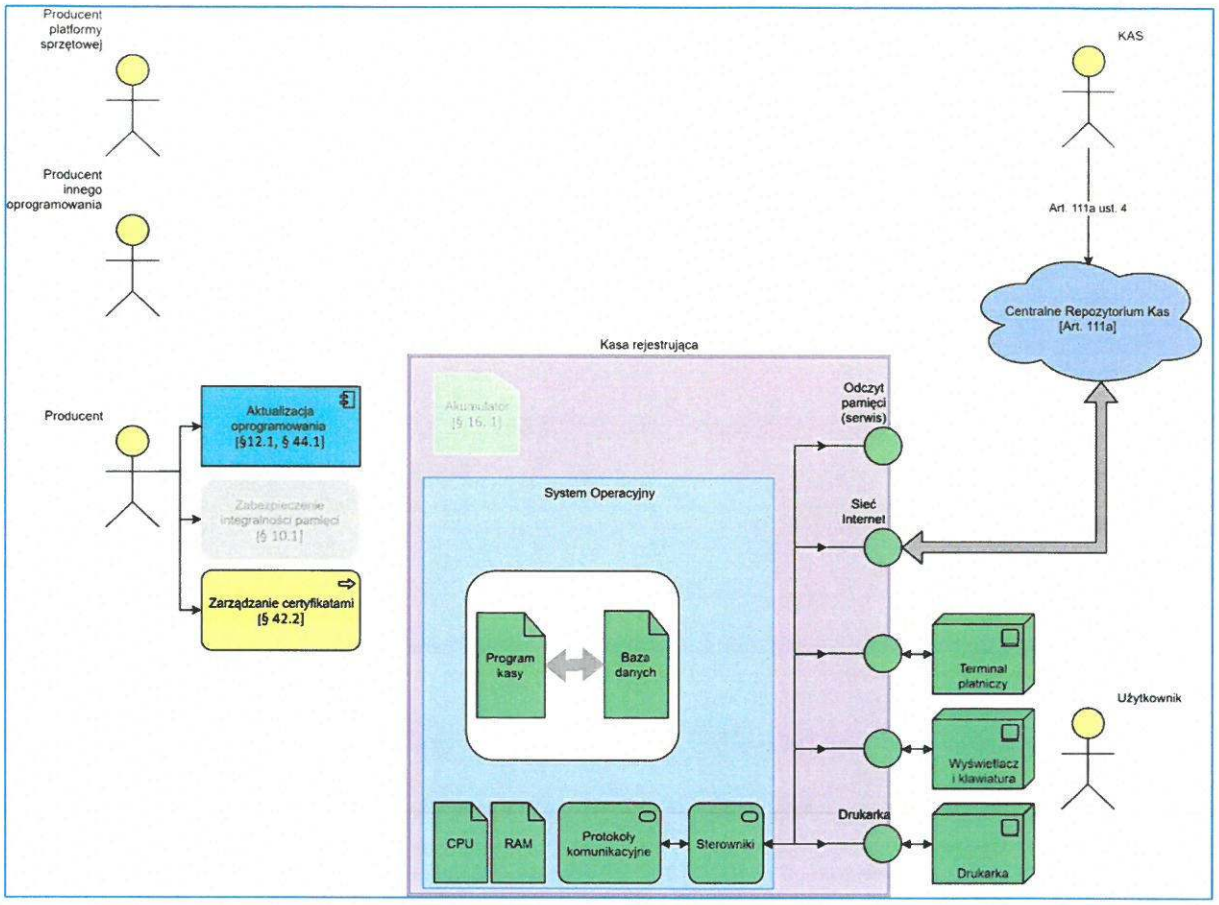


Rysunek 2 Model kasy rejestrującej on-line w wersji sprzętowej.
Źródło: opracowanie własne.

W modelu tym kasa rejestrująca stanowi technologicznie zamknięty ekosystem wspierany organizacyjnie przez kompetentne osoby o określonym zakresie zadań i odpowiedzialności w całym cyklu życia rozwiązania.

4.2. Model kasy rejestrującej zgodnie z Projektem (programowy)

Na podstawie wymagań dotyczących kas rejestrujących określonych w **Projekcie** opracowano poniższy model.



Rysunek 3 Model kasy rejestrującej on-line w wersji oprogramowania.
Źródło: opracowanie własne.

W modelu tym kasa rejestrująca stanowi technologicznie otwarty ekosystem, w którym uczestniczą dodatkowo dwie niezależne grupy organizacji z nieokreślonym w przepisach zakresem zadań i odpowiedzialności, których działania lub zaniechania mają istotny wpływ na funkcjonowanie ekosystemu. Należą do nich.

- Dostawcy platformy sprzętowej stanowią grupę organizacji, która dostarcza platformę sprzętową, oprogramowanie sterujące (ang. *firmware*) oraz system operacyjny. Do grupy tej można zaliczyć np. LG, Huawei lub Samsung wraz z Google (Alphabet) w przypadku telefonu lub tabletu z systemem Android.
- Dostawcy innego oprogramowania stanowią bardzo szeroką grupę organizacji, która instaluje na tej platformie różne oprogramowanie, często trwale zintegrowane, np. LG, Huawei lub Samsung, którzy instalują swoje nakładki systemowe (ang. launcher) czy nakładki operatora np. Orange (ang. branding). Oczywiście z uwagi na otwartość systemu możliwa jest instalacja innego oprogramowania „ze sklepu". Liczba dostępnych pozycji np. w sklepie Google Play liczy kilka milionów.

4.3. Określenie poziomu spełnienie wymagań bezpieczeństwa

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
5.	**Polityki bezpieczeństwa informacji**		**1**	**0**	
5.1.	Kierunki bezpieczeństwa informacji określane przez kierownictwo Cel: Zapewnienie przez kierownictwo wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji, zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami.		1	0	W wyniku zidentyfikowanych braków związanych z Polityką Bezpieczeństwa Informacji w przypadku rozwiązania kas rejestrujących mających postać oprogramowania, istnieje istotne ryzyko nie podejmowania działań na rzecz bezpieczeństwa informacji, które byłyby adekwatne do wymagań biznesowych oraz właściwych norm prawnych i regulacji.
5.1.1.	Polityki bezpieczeństwa informacji	Zbiór polityk bezpieczeństwa informacji powinien być opracowany, zatwierdzony przez kierownictwo, opublikowany i zakomunikowany pracownikom i właściwym stronom zewnętrznym.	F	N	GUM jako jednostka certyfikująca obecne rozwiązania kas rejestrujących (rozwiązania sprzętowe) opracował właściwą politykę bezpieczeństwa dla tego procesu uwzględniającą właściwe normy prawne i regulacje. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w zakresie polityki bezpieczeństwa informacji. W trakcie uzgodnień wspomina się o certyfikacji, ale żaden projekt odpowiedniej regulacji nie został przedłożony.
5.1.2.	Przegląd polityk bezpieczeństwa informacji	Polityki bezpieczeństwa informacji należy poddawać przeglądom w zaplanowanych odstępach czasu lub wtedy, gdy wystąpią istotne zmiany, aby zapewnić, że nadal są właściwe, adekwatne i skuteczne.	F	N	GUM utrzymuje w aktualności właściwą politykę bezpieczeństwa informacji. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w zakresie polityki bezpieczeństwa informacji.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
6.	**Organizacja bezpieczeństwa informacji**		**1**	**0**	
6.1.	Organizacja wewnętrzna Cel: Ustanowić strukturę zarządzania w celu zainicjowania oraz nadzorowania wdrażania i eksploatacji bezpieczeństwa informacji w organizacji.		1	0	W wyniku zidentyfikowanych braków związanych z ustanowieniem adekwatnej struktury zarządzania bezpieczeństwem informacji w przypadku **Projektu** wprowadzenia kas rejestrujących mających postać oprogramowania istnieje istotne ryzyko zapewnienia zasobów niezbędnych dla zainicjowania oraz nadzorowania wdrażania i eksploatacji bezpieczeństwa informacji w tym przypadku.
6.1.1.	Role i odpowiedzialność za bezpieczeństwo informacji	Odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana.	F	P	W przypadku rozwiązania sprzętowego role i odpowiedzialności za bezpieczeństwo informacji są jawnie określone i możliwe do realizacji. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania zidentyfikowane role i odpowiedzialności za bezpieczeństwo informacji są niewystarczające.
6.1.2.	Rozdzielanie obowiązków	Obowiązki i odpowiedzialności pozostające w konflikcie ze sobą należy rozdzielić, celem ograniczenia okazji do nieuprawnionej lub nieumyślnej modyfikacji lub nadużycia aktywów organizacji.	F	N	W przypadku rozwiązania sprzętowego rozdzielenie ról jest wręcz modelowe. Są role związane z budową, oceną skuteczności zabezpieczeń, bieżącą konserwacją i utrzymaniem oraz eksploatacją. Role te są rozdzielone. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania brakuje wymagań w zakresie rozdzielenia ról. Osoba eksploatująca rozwiązanie może również zajmować się jego konfiguracją (nie zidentyfikowano wymagania rozdzielenia tych ról). Roli związanej z niezależną oceną skuteczności zabezpieczeń nie zidentyfikowano.
6.1.3.	Kontakty z organami władzy	Należy utrzymywać stosowne kontakty z właściwymi organami władzy.	F	P	W przypadku rozwiązania sprzętowego określone są zasady komunikacji z organami władzy (MF, GUM). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania powiadomienia ograniczone są do przypadku utraty kasy (§ 13).

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
6.1.4.	Kontakty z grupami zainteresowanych specjalistów	Należy utrzymywać stosowne kontakty z grupami zainteresowanych specjalistów lub innymi specjalistycznymi forami oraz stowarzyszeniami zawodowymi z obszaru bezpieczeństwa.	F	N	Ekosystem certyfikacji stał się swego rodzaju katalizatorem dla powstawania grup zainteresowanych specjalistów. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano żadnych form skłaniających do współdziałania (całkowity brak regulacji rynku poprzez brak wymagań stawianych producentom takich kas - wymagania mają charakter ogólny i nie są niezależnie weryfikowane).
6.1.5.	Bezpieczeństwo informacji w zarządzaniu projektami	Bezpieczeństwo informacji należy uwzględnić w zarządzaniu projektami, niezależnie od rodzaju projektu.	L	N	Obecne regulacje nie narzucają wymagań w zakresie stosowania odpowiednich procedur przez producenta. Obecna praktyka (certyfikacja) ugruntowała stosowanie takich praktyk (chociaż nie zawsze w sposób dojrzały). **Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania nie określa żadnych wymagań w tym zakresie.
6.2.	Urządzenia mobilne i telepraca Cel: Zapewnić bezpieczeństwo telepracy i stosowania urządzeń mobilnych.		1	1	Wyłączenie
6.2.1.	Polityka stosowania urządzeń mobilnych	Należy wprowadzić politykę oraz wspierające ją zabezpieczenia w celu zarządzanie ryzykami, wynikającymi z użytkowania urządzeń mobilnych.	X	X	Nie dotyczy
6.2.2.	Telepraca	Należy wdrożyć politykę oraz wspierające ją zabezpieczenia w celu ochrony informacji pobieranych, przetwarzanych i przechowywanych w miejscach wykonywania telepracy.	X	X	Nie dotyczy

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
7.	**Bezpieczeństwo zasobów ludzkich**		**1**	**0**	
7.1.	Przed zatrudnieniem Cel: Zapewnić, żeby pracownicy i kontrahenci rozumieli swoją odpowiedzialność i byli odpowiednimi kandydatami do wypełnienia ról, do których są przewidziani.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza ryzyko, że zatrudniony pracownik lub kontrahent nie będzie posiadał odpowiednich kwalifikacji do wypełnienia roli, do której jest przewidziany.
7.1.1.	Postępowanie sprawdzające	Historię wszystkich kandydatów do pracy należy zweryfikować zgodnie z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi oraz proporcjonalnie do wymagań biznesowych, klasyfikacji informacji, do których będzie potrzebny dostęp oraz dostrzeżonych ryzyk.	X	X	Nie określono w przepisach - wyłączono z oceny
7.1.2.	Warunki zatrudnienia	Umowy z pracownikami i kontrahentami powinny określać odpowiedzialność stron w obszarze bezpieczeństwa informacji.	F	P	Wymagania informujące o odpowiedzialności związanej z bezpieczeństwem informacji są określone w przepisach. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania określone wymagania z dużym prawdopodobieństwem nie mogą być spełnione - sprzedawca (użytkownik kasy) nie będzie specjalistą w zakresie bezpieczeństwa informacji w zakresie niezbędnym do utrzymania tego rozwiązania; natomiast producenta nikt nie weryfikuje a tzw. programistą można zostać bez odpowiedniego wykształcenia (brak jakichkolwiek wymagań regulacyjnych).
7.2.	Podczas zatrudnienia Cel: Zapewnić, żeby pracownicy i kontrahenci byli świadomi swoich obowiązków dotyczących bezpieczeństwa informacji i wypełniali je.		1	0	W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania istnieje ryzyko, że zatrudniony pracownik lub kontrahent nie będzie aktualizował wiedzy i umiejętności w zakresie niezbędnym do wypełnienia roli, do której jest przewidziany.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
7.2.1.	Odpowiedzialność kierownictwa	Kierownictwo powinno wymagać, aby wszyscy pracownicy i kontrahenci stosowali zasady bezpieczeństwa informacji zgodnie z obowiązującymi w organizacji politykami i procedurami	F	N	Polityki Bezpieczeństwa Informacji sformułowane są na potrzeby certyfikacji (GUM). Osoby uczestniczące w procesie certyfikacji zobowiązane są do stosowania tych polityk. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania de facto polityki bezpieczeństwa informacji nie są wymagane proponowanymi przepisami. Zakres odpowiedzialności wynika wyłącznie z przepisów ogólnych i odnosi się do procedur postępowania, a nie polityk bezpieczeństwa.
7.2.2.	Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji	Wszyscy pracownicy organizacji oraz, w stosownych wypadkach, kontrahenci powinni przejść stosowne kształcenie i szkolenie uświadamiające oraz regularnie otrzymywać aktualizacje polityk i procedur związanych z ich stanowiskiem pracy.	F	N	Szkolenia i działania uświadamiające są obecnie prowadzone w sposób systemowy (GUM). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania de facto polityki bezpieczeństwa informacji nie są wymagane proponowanymi przepisami, a tym samym trudno wymagać aktualizacji wiedzy o nich.
7.2.3.	Postępowanie dyscyplinarne	Postępowanie dyscyplinarne wobec pracowników naruszających zasady bezpieczeństwa informacji należy prowadzić na podstawie ustalonych i przedstawionych im zasad.	X	X	Postępowanie dyscyplinarne jest zależne od uczestników procesu. Nie sformułowano takich wymagań w przepisach, w których odpowiedzialność sprowadzono do nakładania kar administracyjnych.
7.3.	Zakończenie i zmiana zatrudnienia Cel: Zabezpieczyć interesy organizacji w trakcie procesu zmiany lub zakończenia zatrudnienia.		1	0	**Projekt** w zakresie stosowania kas rejestrujących mających postać oprogramowania wprowadza ryzyko, że w chwili zakończenia działalności lub zmiany zatrudnienia po stronie wytwórcy nie wiadomo kto i jakie uprawnienia będzie nadal posiadał i w jaki sposób może to wpłynąć na działanie kas.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
7.3.1.	Zakończenie zatrudnienia lub zmiana zakresu obowiązków	Należy określić i przedstawić pracownikowi lub kontrahentowi, które odpowiedzialności i obowiązki w zakresie bezpieczeństwa informacji pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, a następnie egzekwować je.	F	N	W przypadku zakończenia zatrudnienia (działalności) określona jest w przepisach procedura rozliczenia działalności i zapewnienia ciągłości działania (wskazania następcy w zakresie serwisu). W **Projekcie** w zakresie stosowania kas rejestrujących mających postać oprogramowania nie zidentyfikowano zapisów dotyczących postępowania w przypadku zakończenia działalności wytwórcy oprogramowania.
8.	**Zarządzanie aktywami**		**1**	**0**	
8.1.	Odpowiedzialność za aktywa Cel: Zidentyfikować aktywa organizacji i zdefiniować właściwą odpowiedzialność w dziedzinie ich ochrony.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza istotne ryzyko w zakresie identyfikacji i odpowiedzialności za ochronę aktywów.
8.1.1.	Inwentaryzacja aktywów	Należy zidentyfikować informacje oraz inne aktywa związane z informacją i obiektami przetwarzania informacji, a spis tych wszystkich aktywów powinien być utworzony i utrzymywany.	F	L	Obecne regulacje wymagają prowadzenia pełnej ewidencji aktywów związanych z informacją i obiektami przetwarzania informacji. W **Projekcie** w zakresie stosowania kas rejestrujących mających postać oprogramowania aktywa sprzętowe nie są inwentaryzowane.
8.1.2.	Własność aktywów	Aktywa znajdujące się w ewidencji należy przypisać ich właścicielom.	F	P	Obecne regulacje wymagają prowadzenia pełnej ewidencji aktywów związanych z informacją i obiektami przetwarzania informacji wraz z przypisaniem ich właścicieli. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania aktywa sprzętowe nie są inwentaryzowane. Nie jest określone czyją pozostają własnością i kto za nie odpowiada.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
8.1.3.	Akceptowalne użycie aktywów	Pracownicy i użytkownicy z zewnątrz korzystający z lub mające dostęp do zasobów organizacji powinni być świadomi wymogów bezpieczeństwa informacji dotyczących aktywów organizacji związanych z informacją, infrastrukturą służącą do przetwarzania informacji i zasobami.	F	N	Akceptowalne użycie aktywów jest ściśle związane z rolami. W przypadku rozwiązania sprzętowego rozdzielenie ról jest właściwe. Są role związane z budową, oceną skuteczności zabezpieczeń, bieżącą konserwacją i utrzymaniem oraz eksploatacją. Role te są rozdzielone. Ponadto infrastruktura służąca przetwarzaniu informacji nie może być wykorzystywana do innych celów niż kasa rejestrująca. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania brakuje wymagań w zakresie rozdzielenia ról. Osoba eksploatująca rozwiązanie może również zajmować się jego konfiguracją (nie zidentyfikowano wymagania rozdzielenia tych ról). Roli związanej z niezależną oceną skuteczności zabezpieczeń nie zidentyfikowano. Ponadto **Projekt** pomija całkowicie wymagania dotyczące infrastruktury sprzętowej. Oznacza to, że na tym sprzęcie mogą być zainstalowane różne inne programy, których działania i wpływu na działanie kasy rejestrującej nikt nie badał.
8.1.4.	Zwrot aktywów	Wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia, powinni zwrócić wszystkie posiadane aktywa organizacji.	F	P	Przepisy określają obowiązki w przypadku zakończenia działalności przez podmiot użytkujący kasę rejestrującą. Z uwagi na fizyczny rodzaj eksploatowanych kas rejestrujących, w tym ich zabezpieczeń, znacznie prostszy do wyegzekwowania jest schemat zwrotu aktywów. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie od producenta (ew. serwisanta), natomiast wyegzekwowanie wymagania zwrotu aktywów od użytkownika jest znacznie trudniejsze w realizacji (przez co istnieje ryzyko niewykonania).

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
8.2.	Klasyfikacja informacji Cel: Zapewnić przypisanie informacjom odpowiedniego poziomu ochrony, zgodnego z ich wagą dla organizacji.		1	0	Istnieje istotne ryzyko w zakresie ochrony informacji adekwatnie do ich wagi dla organizacji.
8.2.1.	Klasyfikowanie informacji	Informacje powinny być klasyfikowane z uwzględnieniem wymagań prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację.	F	N	Obowiązujące przepisy kwalifikują informacje przypisując im położenie w pamięci urządzenia (pamięć fiskalna, pamięć chroniona). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
8.2.2.	Oznaczanie informacji	Należy opracować i wdrożyć odpowiedni zbiór procedur oznaczania informacji, zgodnych z przyjętym w organizacji schematem klasyfikacji informacji.	F	N	Obecnie obowiązuje rodzaj "polityki bezpieczeństwa" określającej jakie dane gdzie i w jaki sposób mają być składowane oraz w jaki sposób i dla kogo mają być dostępne. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
8.2.3.	Postępowanie z aktywami	Należy opracować i wdrożyć procedury postępowania z aktywami, zgodnie z przyjętym przez organizację schematem klasyfikacji informacji.	F	N	Obecnie obowiązuje rodzaj "polityki bezpieczeństwa" określającej jakie dane gdzie i w jaki sposób mają być składowane oraz w jaki sposób i dla kogo mają być dostępne, co jest weryfikowane w procesie certyfikacji GUM. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
8.3.	Postępowanie z nośnikami Cel: Zapobiec nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji zapisanych na nośnikach.		1	0	Istnieje ryzyko ujawnienia, modyfikacji, usunięcia lub zniszczenia informacji zapisanych na nośnikach z uwagi na nieprecyzyjne i niespójne uregulowania w **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania.
8.3.1.	Zarządzanie nośnikami wymiennymi	Organizacja powinna wdrożyć procedury zarządzania nośnikami wymiennymi, zgodne ze schematem klasyfikacji przyjętym w organizacji.	F	N	Kasy rejestrujące zgodne z obecnymi przepisami prawa nie posiadają łatwo dostępnych nośników wymiennych. Dostęp do pamięci urządzenia jest opisany szczegółowo w przepisach i jest chroniony. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Pamięci wymienne w przypadku większości platform, na których oprogramowanie to mogłoby być uruchamiane domyślnie nie chroni dostępu do pamięci.
8.3.2.	Wycofywanie nośników	Nośniki, które nie będą dłużej wykorzystywane, należy bezpiecznie wycofać, zgodnie z formalnymi procedurami.	F	N	Obecne regulacje w zakresie postępowania z nośnikami informacji w kasach rejestrujących zapewniają bezpieczne wycofywanie nośników. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
8.3.3.	Przekazywanie nośników	Nośniki zawierające informacje należy chronić przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu.	F	N	Obecne regulacje w zakresie postępowania z nośnikami informacji w kasach rejestrujących zapewniają właściwą ochronę przed nieuprawnionym dostępem, nadużyciem oraz utratą integralności podczas transportu. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
9.	**Kontrola dostępu**		1	0	
9.1.	Wymagania biznesowe wobec kontroli dostępu Cel: Ograniczyć dostęp do informacji i środków przetwarzania informacji.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza istotne ryzyko uzyskania nieuprawnionego dostępu do informacji.
9.1.1.	Polityka kontroli dostępu	Politykę kontroli dostępu należy ustanowić, udokumentować i poddawać przeglądom zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji.	F	N	Obecne regulacje dokładnie określają kto i w jakim trybie posiadać ma dostęp do informacji (polityka kontroli dostępu oparta na rolach). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
9.1.2.	Dostęp do sieci i usług sieciowych	Użytkownicy powinni mieć dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia.	F	N	Obecne regulacje zapewniają, że kasy rejestrujące są systemem zamkniętym certyfikowanym w zakresie bezpieczeństwa przez niezależne laboratorium (GUM). Obecnie kasy rejestrujące mają jedynie dostęp tylko do tych sieci i usług sieciowych do których mają mieć uprawnienia. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. W przypadku większości platform, na których oprogramowanie to mogłoby być uruchamiane domyślnie ich użytkownik ma pełną swobodę w tym zakresie.
9.2.	Zarządzenie dostępem użytkowników Cel: Zapewnić dostęp uprawnionym użytkownikom i zapobiec nieuprawnionemu dostępowi do systemów i usług.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza ryzyko istnienia nieuprawnionego dostępu do systemów i usług.
9.2.1.	Rejestrowanie i wyrejestrowywanie użytkowników	W celu umożliwienia przydzielania praw dostępu należy wdrożyć formalny proces rejestrowania i wyrejestrowywania użytkowników.	F	N	Obecnie istnieje formalny proces rejestrowania i wyrejestrowywania użytkowników z kas rejestrujących. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Wszelkie uprawnienia domyślnie będzie posiadał użytkownik i tylko od jego doświadczenia i potrzeb zależeć będzie konfiguracja.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
9.2.2.	Przydzielanie dostępu użytkownikom	Należy wdrożyć formalny proces przydzielania dostępu użytkownikom w celu nadawania lub odbierania praw dostępu do wszystkich systemów i usług wszystkim kategoriom użytkowników.	F	N	Jak 9.2.2.
9.2.3.	Zarządzanie prawami uprzywilejowanego dostępu	Przydzielanie i wykorzystanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować.	F	N	Prawa uprzywilejowanego dostępu są obecnie ograniczone (zarządzanie dostępem opartym na rolach) i nadzorowane (uprawnienia serwisu, konieczności dokonywania wpisów, plomb). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Domyślnie na większości platform ich właściciel (użytkownik kasy) będzie dysponował uprzywilejowanym dostępem.
9.2.4.	Zarządzanie poufnymi informacjami uwierzytelniającymi użytkowników	Przydzielanie poufnych informacji uwierzytelniających powinno podlegać formalnemu procesowi zarządzania.	F	N	Obecne regulacje promują dobre praktyki w tym zakresie, w szczególności w zakresie dostępu do kont uprzywilejowanych (serwis). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
9.2.5.	Przegląd praw dostępu użytkowników	Właściciele aktywów powinni przeglądać prawa dostępu użytkowników w regularnych odstępach czasu.	L	N	Przegląd praw dostępu użytkowników może nie być prowadzony przez właścicieli kas rejestrujących. Konta uprzywilejowane są kontrolowane niezależnie. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
9.2.6.	Odbieranie lub dostosowywanie praw dostępu	Przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do informacji i środków przetwarzania informacji należy odbierać po zakończeniu zatrudnienia, umowy lub porozumienia lub dostosowywać do zaistniałych zmian.	F	N	Istnieją obecnie formalne wymagania w zakresie odbierania lub dostosowywania praw dostępu. Wszelkie zmiany są rejestrowane. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
9.3.	Odpowiedzialność użytkowników Cel: Zapewnić rozliczalność użytkowników w celu ochrony ich informacji uwierzytelniających.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza istotne ryzyko, że informacje uwierzytelniające zostaną ujawnione osobom trzecim.
9.3.1.	Stosowanie poufnych informacji uwierzytelniających	Użytkownicy powinni mieć obowiązek przestrzegania przyjętych w organizacji zasad stosowania poufnych informacji uwierzytelniających.	L	N	Istnieją obecnie formalne wymagania w zakresie zasad stosowania poufnych informacji uwierzytelniających. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
9.4.	Kontrola dostępu do systemów i aplikacji Cel: Zapobiec nieuprawnionemu dostępowi do systemów i aplikacji.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza istotne ryzyko uzyskania nieuprawnionego dostępu do systemów i aplikacji.
9.4.1.	Ograniczanie dostępu do informacji	Dostęp do informacji oraz funkcji systemu aplikacyjnego należy ograniczać zgodnie z polityką kontroli dostępu.	F	N	Istnieje obecnie formalna polityka kontroli dostępu weryfikowana w procesie certyfikacji kasy rejestrującej. W **Projekcie** dotyczącym wprowadzenia stosowania kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
9.4.2.	Procedury bezpiecznego logowania	Tam, gdzie polityka kontroli dostępu tego wymaga, dostęp do systemów i aplikacji powinien być kontrolowany przez procedurę bezpiecznego logowania.	F	N	Jak 9.4.1.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
9.4.3.	System zarządzania hasłami	Systemy zarządzania hasłami powinny być interaktywne i zapewniać wybór haseł dobrej jakości.	X	X	Brak regulacji - wyłączenie. Wymaganie może być trudne w realizacji (nieakceptowane). Istnieją obecnie inne silne formy uwierzytelnienia (wymagania zdjęcia obudowy i zerwania zabezpieczeń, a po zakończeniu pracy ich założenia.
9.4.4.	Użycie uprzywilejowanych programów narzędziowych	Wykorzystanie programów narzędziowych, umożliwiających obejście zabezpieczeń systemów i aplikacji, powinno podlegać ograniczeniom i ścisłemu nadzorowi.	F	N	Użycie programów narzędziowych możliwe jest obecnie jedynie przez pracowników serwisu. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Domyślnie platformy, na których możliwe jest uruchomienie takiego oprogramowania nie kontrolują tego aspektu.
9.4.5.	Kontrola dostępu do kodów źródłowych programów	Dostęp do kodu źródłowego programów powinien być ograniczony.	F	N	Kod źródłowy jest w pełni kontrolowany przez producenta. Jest elementem certyfikacji. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie, chociaż w procesie uzgodnieniowym pojawia się informacja o takich planach.
10.	**Kryptografia**		**1**	**0**	
10.1.	Zabezpieczenia kryptograficzne Cel: Zapewnić właściwe i skuteczne wykorzystanie kryptografii do ochrony poufności, autentyczności i/lub integralności informacji.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza istotne ryzyko dla właściwego i skutecznego wykorzystania kryptografii do ochrony poufności, autentyczności i/lub integralności informacji.
10.1.1.	Polityka stosowania zabezpieczeń kryptograficznych	Należy opracować i wdrożyć politykę stosowania zabezpieczeń kryptograficznych do ochrony informacji.	L	L	Polityka stosowania zabezpieczeń kryptograficznych jest elementem regulacji. Dyskusyjny może być 10 letni okres ważności klucza producenta w **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
10.1.2.	Zarządzanie kluczami	Należy opracować politykę dotyczącą korzystania, ochrony i okresów ważności kluczy kryptograficznych i wdrożyć ją na wszystkich etapach cyklu życia kluczy.	F	N	W przypadku obecnej regulacji klucze przechowywane są w module kryptograficznym chronionej kasy i go nie opuszczają (standard TPM co najmniej w wersji 2). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
11.	**Bezpieczeństwo fizyczne i środowiskowe**		1	0	
11.1.	Obszary bezpieczne Cel: Zapobiec nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach i środkach przetwarzania informacji należących do organizacji.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza istotne ryzyko naruszenia obszaru bezpiecznego.
11.1.1.	Fizyczna granica obszaru bezpiecznego	Należy określić granice bezpieczeństwa i wykorzystać je do zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje oraz środki przetwarzania informacji.	F	N	Fizyczna granica obszaru bezpiecznego została określona obecnie dla urządzenia. Urządzenie jest chronione przed nieupoważnionym dostępem. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
11.1.2.	Fizyczne zabezpieczenie wejść	Bezpieczne strefy należy chronić odpowiednimi zabezpieczeniami wejść zapewniającymi dostęp wyłącznie osobom uprawnionym.	X	X	Wyłączenie - zabezpieczenie nie ma zastosowania.
11.1.3.	Zabezpieczenie biur, pomieszczeń i obiektów	Należy zaprojektować i stosować fizyczne zabezpieczenia biur, pomieszczeń i obiektów.	F	N	Obecnie urządzenia kas rejestrujących są fizycznie zabezpieczone przed nieuprawnionym dostępem. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
11.1.4.	Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi	Należy zaprojektować i stosować fizyczne zabezpieczenia przed katastrofami naturalnymi, wrogim atakiem lub wypadkami.	F	N	Obecnie urządzenia kas rejestrujących są fizycznie zabezpieczone przed zagrożeniami zewnętrznymi i środowiskowymi (certyfikacja). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
11.1.5.	Praca w obszarach bezpiecznych	Należy zaprojektować i stosować procedury pracy w obszarach bezpiecznych.	F	N	Zaprojektowano w przepisach zasady prowadzenia serwisu (praca w obszarze bezpiecznym). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
11.1.6.	Obszary dostaw i załadunku	Należy sprawować nadzór nad punktami dostępu takimi jak obszary dostaw i załadunku oraz innymi punktami, przez które nieuprawnione osoby mogą wejść do pomieszczeń, i, jeśli to możliwe, odizolować je od środków przetwarzania informacji, aby zapobiec nieuprawnionemu dostępowi.	X	X	Wyłączenia - zabezpieczenie nie ma zastosowania.
11.2.	Sprzęt Cel: Zapobiec utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza ryzyko w zakresie możliwości utraty, uszkodzenia, kradzieży lub utraty integralności aktywów i wystąpienia zakłóceń w działaniu.
11.2.1.	Lokalizacja i ochrona sprzętu	Sprzęt należy umieścić i chronić w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu.	F	N	Obecne regulacje zapewniają, że kasy rejestrujące są systemem zamkniętym certyfikowanym w zakresie bezpieczeństwa przez niezależne laboratorium (GUM). Obecnie kasy rejestrujące mają odpowiednie zabezpieczenia fizyczne przed nieuprawnionym dostępem. W Projekcie dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano żadnych wymagań w tym zakresie.
11.2.2.	Systemy wspomagające	Sprzęt należy chronić przez awariami zasilania oraz innymi przerwami spowodowanymi awariami systemów wspomagających.	F	N	Obecne regulacje wymagają instalacji akumulatora zapewniającego możliwość działania i odporność na przerwy w zasilaniu. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
11.2.3.	Bezpieczeństwo okablowania	Okablowanie zasilające oraz telekomunikacyjne, przenoszące dane lub wspomagające usługi informacyjne należy chronić przed przechwyceniem, zakłóceniem lub uszkodzeniem.	F	N	Obecnie wymagania w zakresie komunikacji kasy z peryferiami (drukarka) są określone i weryfikowane w trakcie certyfikacji. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Należy zauważyć, że z uwagi na korzystanie z niekontrolowanego środowiska możliwych platform technicznych istnieje możliwość przechwycenia i modyfikacji transmisji narzędziami systemowymi (np. wydruk do PDF, drukowanie z innych aplikacji, itp.).
11.2.4.	Konserwacja sprzętu	Sprzęt należy prawidłowo konserwować w celu zapewnienia jego ciągłej dostępności i integralności.	F	N	Obecnie warunki konserwacji sprzętu są jasno określone i podlegają weryfikacji. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
11.2.5.	Wynoszenie aktywów	Sprzętu, informacji i programów nie należy wynosić poza siedzibę organizacji bez uzyskania wcześniejszego zezwolenia.	X	X	Wyłączenie - zabezpieczenie nie ma zastosowania.
11.2.6.	Bezpieczeństwo sprzętu i aktywów poza siedzibą	Aktywa wynoszone poza siedzibę organizacji należy zabezpieczyć przed wystąpieniem różnych ryzyk związanych z pracą poza siedzibą.	X	X	Wyłączenie - zabezpieczenie nie ma zastosowania.
11.2.7.	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	Przed zbyciem lub przekazaniem sprzętu do ponownego użycia należy sprawdzić wszystkie jego składniki zawierające nośniki informacji, dla zapewnienia, że wszystkie wrażliwe dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.	F	N	Obecnie kasy rejestrujące stanowią zamknięty system, który jest regularnie serwisowany i utrzymywany. Istnieją procedury bezpiecznego zbywania lub przekazywania do ponownego użycia. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
11.2.8.	Pozostawianie sprzętu użytkownika bez opieki	Użytkownicy powinni zapewnić odpowiednią ochronę sprzętu pozostawianego bez opieki.	F	N	Obecnie kasy rejestrujące mają taką funkcjonalność. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Należy zauważyć, że platforma wykorzystywana przez oprogramowanie pełniące funkcję kas rejestrujących może być używana do innych nieznanych zadań. Nie wiadomo, czy i jaki wpływ będzie miało to użytkowanie na funkcję kasy rejestrującej.
11.2.9.	Polityka czystego biurka i czystego ekranu	Należy wprowadzić politykę czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz politykę czystego ekranu dla środków przetwarzania informacji.	X	X	Wyłączenie - zabezpieczenie nie ma zastosowania.
12.	**Bezpieczna eksploatacja**		**1**	**0**	
12.1.	Procedury eksploatacyjne i odpowiedzialność Cel: Zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji.		1	0	**Projekt** dotyczący wprowadzenia stosowania kas rejestrujących mających postać oprogramowania wprowadza istotne ryzyko dla zapewnienia poprawnej i bezpiecznej eksploatacji środków przetwarzania informacji.
12.1.1.	Dokumentowanie procedur eksploatacyjnych	Procedury eksploatacyjne powinny być udokumentowane i udostępniane wszystkim potrzebującym ich użytkownikom.	F	N	Obecnie serwis kas rejestrujących posiada udokumentowane procedury eksploatacyjne pozwalające na bezpieczną eksploatację. W Projekcie dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
12.1.2.	Zarządzanie zmianami	Zmiany w organizacji, procesach biznesowych, środkach przetwarzania informacji i systemach, które mają wpływ na bezpieczeństwo informacji, powinny być nadzorowane.	F	N	Obecnie jest uregulowany, formalny procesu zarządzania zmianą obejmujący wszystkie komponenty systemu mające wpływ na bezpieczeństwo informacji. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Jednocześnie należy zauważyć, że zarządzanie zmianą systemem operacyjnym i innymi komponentami platformy, na której może być instalowane oprogramowanie (zgodnie z **Projektem**) jest w praktyce poza kontrolą.
12.1.3.	Zarządzanie pojemnością	Należy monitorować i dostosowywać wykorzystanie zasobów oraz przewidywać wymaganą pojemność w przyszłości, dla zapewnienia właściwej wydajności systemu.	F	N	Obecnie pojemność jest w pełni monitorowana i właściwe działania korygujące są przewidziane i zaplanowane. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Jednocześnie należy zauważyć, że zarządzanie systemem operacyjnym i innymi komponentami platformy, na której może być instalowane oprogramowanie (zgodnie z **Projektem**) jest w praktyce poza kontrolą. Może to skutkować niekontrolowaną utylizacją zasobów platformy, co zdestabilizuje pracę kasy rejestrującej mającej postać oprogramowania.
12.1.4.	Oddzielanie środowisk rozwojowych, testowych i produkcyjnych	Należy oddzielić środowiska rozwojowe, testowe i produkcyjne celem redukcji ryzyk związanych z nieuprawnionym dostępem lub zmianami w środowisku produkcyjnym.	F	N	Obecnie środowiska te są w pełni rozdzielone. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
12.2.	Ochrona przed szkodliwym oprogramowaniem Cel: Zapewnić informacjom i środkom przetwarzania informacji ochronę przed szkodliwym oprogramowaniem.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza ryzyko nieadekwatnej ochrony przed szkodliwym oprogramowaniem.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
12.2.1.	Zabezpieczenia przed szkodliwym oprogramowaniem	Należy wdrożyć zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników.	F	N	Obecnie cały ekosystem kasy rejestrującej jest systemem zamkniętym. Odpowiednie zabezpieczenia są wdrożone po stronie producenta. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Jednocześnie należy zauważyć, że zarządzanie systemem operacyjnym i innymi komponentami platformy, na której może być instalowane oprogramowanie (zgodnie z **Projektem**) jest w praktyce poza kontrolą. Może to skutkować niekontrolowaną instalacją szkodliwego oprogramowania (powszechnie dostępnego na te platformy), co zdestabilizuje pracę kasy rejestrującej mającej postać oprogramowania.
12.3.	Kopie zapasowe Cel: Chronić przed utratą danych.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza ryzyko utraty danych.
12.3.1.	Zapasowe kopie informacji	Zapasowe kopie informacji, oprogramowania i obrazów systemów należy regularnie wykonywać i testować, zgodnie z ustaloną polityką kopii zapasowych.	F	P	Obecnie wydzielone są obszary pamięci chronione w sposób skutecznie zabezpieczające przed utratą danych. W przypadku nowelizacji w zakresie stosowania kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Funkcja zapewniająca przesyłanie danych na serwery Ministerstwa Finansów nie jest w tym przypadku wystarczająco skuteczna (kasa może pracować off-line).
12.4.	Rejestrowanie zdarzeń i monitorowanie Cel: Rejestrować zdarzenia i zbierać materiał dowodowy.		1	0	Istnieje ryzyko utraty manipulacji rejestrem zdarzeń w przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
12.4.1.	Rejestrowanie zdarzeń	Należy tworzyć, przechowywać i systematycznie przeglądać dzienniki zdarzeń rejestrujące działania użytkowników, wyjątki, usterki oraz zdarzenia związane z bezpieczeństwem informacji.	F	N	Dzienniki zdarzeń są wdrożone. Tworzone w ten sposób zapisy nie mogą być modyfikowane (usuwane) celowo np. w przypadku skutecznego przełamania zabezpieczeń, a prawdopodobieństwo utraty w przypadku awarii albo wyłączenia zasilania jest bardzo nikłe. Polityka dotycząca zakresu zbieranych informacji oraz sposobu ich przeglądania, analizy oraz podejmowania dalszych działań na tej podstawie jest jasna. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Ponadto platforma techniczna do instalacji tego oprogramowania bez specjalnego przygotowania nie zapewnia tej funkcjonalności.
12.4.2.	Ochrona informacji w dziennikach zdarzeń	Środki służące rejestrowaniu zdarzeń oraz informacje w dziennikach zdarzeń należy chronić przed manipulacją i nieuprawnionym dostępem..	F	N	W przypadku obecnej regulacji występuje pełna ochrona informacji zawartych w dziennikach zdarzeń w zakresie konstrukcyjnym oraz podziale ról i uprawnień. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
12.4.3.	Rejestrowanie działań administratorów i operatorów	Działania administratorów i operatorów systemów należy rejestrować, a dzienniki chronić i systematycznie przeglądać.	F	N	W przypadku obecnej regulacji jest zachowana pełna identyfikowalność (również rejestr papierowy). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
12.4.4.	Synchronizacja zegarów	Zegary wszystkich istotnych systemów przetwarzania informacji w organizacji lub domenie bezpieczeństwa należy zsynchronizować z jednym wzorcowym źródłem czasu.	F	P	W przypadku obecnej regulacji moduł zegara czasu rzeczywistego jest obowiązkowym wyposażeniem każdej kasy rejestrującej. Czas jest kontrolowany. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Dostępne do instalacji takiego oprogramowania platformy posiadają funkcjonalność czasu rzeczywistego, jednak może on być manipulowany przez użytkownika bez jakiejkolwiek kontroli.
12.5.	Nadzór nad oprogramowaniem produkcyjnym Cel: Zapewnić integralność systemów produkcyjnych.		1	0	Istnieje istotne ryzyko naruszenia integralności systemów produkcyjnych w przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania.
12.5.1.	Instalacja oprogramowania w systemach produkcyjnych	Należy wdrożyć procedury nadzoru nad instalacją oprogramowania w systemach produkcyjnych.	F	N	W przypadku obecnej regulacji istnieją mechanizmy skutecznej kontroli instalacji oprogramowania w kasach rejestrujących. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Ponadto platforma techniczna do instalacji tego oprogramowania bez specjalnego przygotowania nie zapewnia tej funkcjonalności.
12.6.	Zarządzanie podatnościami technicznymi Cel: Zapobiec wykorzystywaniu podatności technicznych.		1	0	Istnieje bardzo duże ryzyko wykorzystania istniejących podatności technicznych w przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
12.6.1.	Zarządzanie podatnościami technicznymi	Informacje o podatnościach technicznych wykorzystywanych systemów informacyjnych należy niezwłocznie pozyskiwać, oceniać stopień narażenia organizacji na te podatności i podejmować odpowiednie środki w celu przeciwdziałania związanemu z nimi ryzyku.	F	N	W przypadku obecnej regulacji istnieją mechanizmy skutecznego zarządzania podatnościami technicznymi w kasach rejestrujących. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Ponadto platforma techniczna do instalacji tego oprogramowania bez specjalnego jej przygotowania (konfiguracji lub modyfikacji) nie zapewnia tej funkcjonalności.
12.6.2.	Ograniczenia w instalowaniu oprogramowania	Należy ustanowić i wdrożyć zasady instalowania oprogramowania przez użytkowników.	F	N	Obecnie określone są jasne zasady dopuszczające lub zabraniające instalacji oprogramowania (realizuje je wykwalifikowany serwis). Generalną praktyką jest ograniczenie uprawnień administratora (serwisu) co ogranicza możliwość instalacji oprogramowania przez użytkowników. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Ponadto platforma techniczna do instalacji tego oprogramowania bez specjalnego jej przygotowania (konfiguracji lub modyfikacji) nie zapewnia tej funkcjonalności.
12.7.	Rozważania dotyczące audytu systemów informacyjnych Cel: Zminimalizować wpływ działań audytu na systemy produkcyjne.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza ryzyko negatywnego wpływu działań audytu na systemy produkcyjne.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
12.7.1.	Zabezpieczenia audytu systemów informacyjnych	Należy starannie zaplanować i uzgodnić wymagania audytu oraz działania obejmujące weryfikację systemów produkcyjnych, w celu zminimalizowania zakłóceń w procesach biznesowych.	F	N	Obecnie odpowiednikiem audytu są: - działania certyfikacyjne prowadzone przez GUM oraz - kontrole prowadzone przez organy skarbowe. Osoby prowadzące te działania są właściwie przygotowane do prowadzenia badania oraz serwisu co ogranicza możliwość instalacji oprogramowania przez użytkowników. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Z uwagi na wielość dostępnych platform i różnice w obsłudze oprogramowania, organy skarbowe na dzień dzisiejszy nie są i prawdopodobnie nie będą odpowiednio przygotowane do wykonywania tych kontroli (audytów). Pozostałe działania kontrolne (GUM) nie są planowane/dopuszczone.
13.	**Bezpieczeństwo komunikacji**		**1**	**0**	
13.1.	Zarządzanie bezpieczeństwem sieci Cel: Zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania informacji.		1	0	**Projekt** dotyczący wprowadzenia kas rejestrujących mających postać oprogramowania wprowadza ryzyko negatywnego wpływu sieci na bezpieczeństwo informacji.
13.1.1.	Zabezpieczenia sieci	Sieci powinny być zarządzane i nadzorowane, w celu ochrony informacji w systemach i aplikacjach.	F	N	Obecnie usługi sieciowe są pod pełną kontrolą dostawcy rozwiązania (rozwiązanie zamknięte). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Platformy techniczne są na tyle otwarte, że ich konfiguracja jest w praktyce poza kontrolą.
13.1.2.	Bezpieczeństwo usług sieciowych	Umowy dotyczące wszystkich usług sieciowych, świadczonych wewnętrznie lub zlecanych na zewnątrz, powinny zawierać zidentyfikowane mechanizmy zabezpieczeń, poziomy świadczenia usług i wymagania dotyczące zarządzania.	F	P	Obecnie usługi sieciowe są pod pełną kontrolą dostawcy rozwiązania (rozwiązanie zamknięte) a transmisja danych jest szyfrowana. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania zidentyfikowano wymagania wyłącznie w zakresie szyfrowania w architekturze PKI. Platformy techniczne są na tyle otwarte, że ich konfiguracja jest w praktyce poza kontrolą.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
13.1.3.	Rozdzielanie sieci	Grupy usług informacyjnych, użytkowników i systemów informacyjnych powinny być rozdzielone w strukturze sieci.	X	X	Wyłączenie - zabezpieczenie nie ma zastosowania.
13.2.	Przesyłanie informacji Cel: Utrzymać bezpieczeństwo informacji przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi.		1	1	Zminimalizowano ryzyko dla bezpieczeństwa informacji przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi.
13.2.1.	Polityki i procedury przesyłania informacji	Należy wdrożyć formalne polityki przesyłania informacji, procedury i zabezpieczenia w celu ochrony wymiany informacji przesyłanych przy użyciu wszystkich rodzajów środków łączności.	F	F	Są określone w przepisach a **Projekt** ich nie zmienia.
13.2.2.	Porozumienia dotyczące przesyłania informacji	Porozumienia powinny uwzględniać bezpieczne przesyłanie informacji biznesowych między organizacją i podmiotami zewnętrznymi.	F	F	Są określone w przepisach a **Projekt** ich nie zmienia.
13.2.3.	Wiadomości elektroniczne	Informacje przekazywane w formie wiadomości elektronicznych powinny być odpowiednio chronione.	F	F	Są określone w przepisach a **Projekt** ich nie zmienia.
13.2.4.	Umowy o zachowaniu poufności	Należy zidentyfikować, regularnie przeglądać i dokumentować wymagania odnoszące się do umów o zachowaniu poufności lub nieujawnianiu informacji, w sposób odzwierciedlający potrzeby organizacji w zakresie ochrony informacji.	F	F	Są określone w przepisach a **Projekt** ich nie zmienia.
14.	**Pozyskiwanie, rozwój i utrzymanie systemów**		**1**	**0**	

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
14.1.	Wymagania związane z bezpieczeństwem systemów informacyjnych Cel: Zapewnić, żeby bezpieczeństwo informacji było nieodłączną częścią systemów informacyjnych w całym cyklu życia. Dotyczy to również wymagań wobec systemów informacyjnych dostarczających usług w sieciach publicznych.		1	0	Istnieje ryzyko dla bezpieczeństwa informacji w przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania z uwagi na fragmentaryczność rozwiązania (nie uwzględniono wszystkich elementów systemu w ramach regulacji).
14.1.1.	Analiza i specyfikacja wymagań bezpieczeństwa informacji	Wymagania dotyczące bezpieczeństwa informacji należy włączyć do wymagań stawianych nowym systemom informacyjnym lub rozbudowie systemów istniejących.	F	N	Obecny stan prawny reguluje wymagania w zakresie bezpieczeństwa w sposób kompleksowy. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie wobec wszystkich komponentów systemu (fragmentaryczność) oraz wszystkich aspektów czasu życia.
14.1.2.	Zabezpieczanie usług aplikacyjnych w sieciach publicznych	Informacje przesyłane w sieciach publicznych, związane z usługami świadczonymi przez aplikacje, należy chronić przed nieuczciwymi działaniami, sporami dotyczącymi umów oraz nieuprawnionym ujawnieniem i zmianami.	F	L	Usługi aplikacyjne w sieciach publicznych są chronione w stopniu wystarczającym. W **Projekcie** dotyczącym wprowadzenia stosowania kas rejestrujących mających postać oprogramowania istnieją ryzyka nieuczciwych działań (brak kontroli nad stosem protokołów komunikacyjnych oraz miejscem przechowywania i sposobem zarządzania certyfikatami cyfrowymi służącymi zabezpieczeniu transmisji).
14.1.3.	Ochrona transakcji usług aplikacyjnych	Informacje związane z transakcjami dokonywanymi w ramach usług świadczonych przez aplikacje należy chronić, aby zapobiec przerwaniu transmisji, błędom w trasowaniu, nieuprawnionym zmianom wiadomości, nieuprawnionemu ujawnieniu, nieuprawnionemu powieleniu lub odtworzeniu.	F	P	Kasy rejestrujące zgodne z obecnymi przepisami prawa są urządzeniami zamkniętymi i testowanymi pod kątem ochrony transakcji usług aplikacyjnych. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania istnieją ryzyka nieuczciwych działań (brak kontroli nad stosem protokołów komunikacyjnych skutkującym możliwością wpływania na przerwy w transmisji, błędy trasowania, zmiany wiadomości, czy nieuprawnionemu powieleniu/odtworzeniu).

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
14.2.	Bezpieczeństwo w procesach rozwoju i wsparcia Cel: Zapewnić projektowanie i wdrożenie bezpieczeństwa informacji w ramach cyklu życia systemów informacyjnych.		1	0	W przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania istnieje ryzyko negatywnego wpływu procesów rozwoju i wsparcia na bezpieczeństwo informacji.
14.2.1.	Polityka bezpieczeństwa prac rozwojowych	Należy ustanowić zasady prac nad rozwojem oprogramowania i systemów oraz stosować je w pracach rozwojowych prowadzonych wewnątrz organizacji.	F	N	Zasady prac nad rozwojem oprogramowania i systemów kas rejestrujących są obecnie uregulowane. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
14.2.2.	Procedury kontroli zmian w systemach	Należy nadzorować zmiany w systemach podczas ich cyklu rozwojowego, przy użyciu formalnych procedur kontroli zmian.	F	N	Zasady kontroli zmian w systemach kas rejestrujących są obecnie uregulowane. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
14.2.3.	Przegląd techniczny aplikacji po zmianach w platformie produkcyjnej	Po dokonaniu zmian w platformach produkcyjnych należy przeprowadzić przegląd krytycznych aplikacji biznesowych oraz przetestować je, aby uzyskać pewność, że zmiany nie miały niekorzystnego wpływu na działalność organizacji lub bezpieczeństwo.	F	N	Zasady dotyczące prowadzenia przeglądu technicznego aplikacji w systemach kas rejestrujących po wprowadzeniu zmian są obecnie uregulowane. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
14.2.4.	Ograniczenia dotyczące zmian w pakietach oprogramowania	Modyfikacji w pakietach oprogramowania należy dokonywać z rozwagą i ograniczać się do zmian niezbędnych, a wszystkie takie zmiany ściśle nadzorować.	F	N	Obecnie zmiany w pakietach oprogramowania kas rejestrujących są pod pełną kontrolą odpowiednio przygotowanych osób. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Ponadto platformy techniczne, które mogą być wykorzystane do działania tego oprogramowania są na tyle elastyczne, że umożliwiają dokonywanie tych zmian praktycznie bez kontroli.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
14.2.5.	Zasady projektowania bezpiecznych systemów	Należy ustanowić, udokumentować i utrzymywać zasady projektowania bezpiecznych systemów oraz stosować je do wszystkich prac implementacyjnych nad systemami informacyjnymi.	F	N	Obecnie, producenci kas rejestrujących z uwagi na konieczność niezależnej certyfikacji (GUM) wypracowali skuteczne zasady projektowania bezpiecznych systemów. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
14.2.6.	Bezpieczne środowisko rozwojowe	Organizacje powinny ustanowić i odpowiednio chronić bezpieczne środowiska rozwojowe przeznaczone do rozwoju systemów oraz prac integracyjnych obejmujących całość cyklu rozwojowego systemów.	F	N	Obecnie producenci kas rejestrujących dysponują właściwie przygotowanym wydzielonym środowiskiem (doświadczenie). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
14.2.7.	Prace rozwojowe zlecane podmiotom zewnętrznym	Organizacja powinna nadzorować i monitorować prace rozwojowe nad systemami zlecone podmiotom zewnętrznym.	F	N	Obecnie producenci kas rejestrujących ponoszą całkowitą odpowiedzialność za poprawność działania kas rejestrujących (doświadczenie, sprawdzeni kooperanci). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
14.2.8.	Testowanie bezpieczeństwa systemów	Funkcje bezpieczeństwa należy testować w czasie prac rozwojowych.	F	N	Obecnie testowanie bezpieczeństwa systemów są prowadzone w celu przygotowania produktu do certyfikacji (GUM). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
14.2.9.	Testy akceptacyjne systemów	Dla nowych systemów informacyjnych, ich modernizacji i nowych wersji systemów należy ustanowić programy testów akceptacyjnych i kryteria z nimi związane.	F	N	Obecnie testowanie akceptacyjne systemów przez niezależną jednostkę certyfikującą jest wymogiem (GUM). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
14.3.	Dane testowe Cel: Zapewnić ochronę danych stosowanych do testów.		1	0	W przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania istnieje ryzyko nieadekwatnej ochrony danych testowych.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
14.3.1.	Ochrona danych testowych	Dane testowe należy starannie wybierać, chronić i nadzorować.	F	N	Ochrona danych testowych jest elementem certyfikacji (GUM). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
15.	**Relacje z dostawcami**		**1**	**0**	
15.1.	Bezpieczeństwo informacji w relacjach z dostawcami Cel: Zapewnić ochronę aktywów organizacji udostępnianych dostawcom.		1	0	W przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania istnieje ryzyko nieadekwatnej ochrony aktywów organizacji udostępnionych dostawcom.
15.1.1.	Polityka bezpieczeństwa informacji w relacjach z dostawcami	Należy uzgodnić z dostawcą i udokumentować wymagania bezpieczeństwa informacji celem zmniejszenia ryzyk związanych z dostępem dostawcy do aktywów organizacji.	F	N	Obowiązujące przepisy zapewniają właściwie udokumentowaną odpowiedzialność wszystkich stron (łącznie z podwykonawcami dostawcy/producenta). W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie (są częściowe, lecz nie dotyczą wszystkich składników systemu, np. oprogramowania systemowego).
15.1.2.	Uwzględnianie bezpieczeństwa w porozumieniach z dostawcami	Należy ustanowić wszystkie istotne wymagania dotyczące bezpieczeństwa informacji i uzgodnić je z każdym dostawcą, który może uzyskać dostęp, przetwarzać, przechowywać, przesyłać lub dostarczać elementy infrastruktury teleinformatycznej dla przetwarzania informacji należących do organizacji.	F	N	jw. W szczególności wielu dostawców systemów operacyjnych prowadzi tzw. telemetrię pobierając wiele informacji o stanie urządzenia. Domyślnie wiele informacji jest lub może być przekazywanych, a użytkownik często nie posiada wiedzy w celu właściwej konfiguracji platformy.
15.1.3.	Łańcuch dostaw technologii informacyjnych i telekomunikacyjnych	Porozumienia z dostawcami powinny uwzględniać wymagania odnoszące się do ryzyk w bezpieczeństwie informacji, związanych z usługami technologii informacyjnych i telekomunikacyjnych oraz łańcuchem dostaw produktów.	F	N	Obowiązujące przepisy uwzględniają łańcuch dostaw. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie (są częściowe, lecz nie dotyczą wszystkich składników systemu, np. oprogramowania systemowego).

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
15.2.	Zarządzanie usługami świadczonymi przez dostawców Cel: Utrzymać uzgodniony poziom bezpieczeństwa informacji i świadczonych usług zgodnie z umowami z dostawcami.		1	0	W przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania istnieje ryzyko utrzymywania poziomu usług nieadekwatnego do faktycznych potrzeb organizacji.
15.2.1.	Monitorowanie i przegląd usług świadczonych przez dostawców	Organizacje powinny regularnie monitorować, przeglądać i audytować dostarczanie usług zewnętrznych.	F	N	Monitorowanie usług dostarczanych przez dostawców oparte jest na wymaganiach określonych w przepisach dla prowadzenia prac serwisowych/konserwacyjnych. W Projekcie dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
15.2.2.	Zarządzenie zmianami w usługach świadczonych przez dostawców	Należy zarządzać zmianami w zakresie świadczenia usług przez dostawców, w tym utrzymaniem i doskonaleniem istniejących polityk bezpieczeństwa informacji, procedur i zabezpieczeń, z uwzględnieniem krytyczności informacji, systemów i procesów biznesowych, których dotyczą oraz ponownego szacowania ryzyka.	F	N	Obecne przepisy regulują kwestie zmian w zakresie świadczonych usług serwisowych/konserwacyjnych. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
16.	**Zarządzanie incydentami związanymi z bezpieczeństwem informacji**		**0**	**0**	
16.1.	Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami Cel: Zapewnić spójne i skuteczne podejście do zarządzania incydentami związanymi z bezpieczeństwem informacji, z uwzględnieniem informowania o zdarzeniach i słabościach.		0	0	Istnieje istotne ryzyko niespójnego i nieskutecznego zarządzania incydentami związanymi z bezpieczeństwem informacji.
16.1.1.	Odpowiedzialność i procedury	Należy ustanowić odpowiedzialność kierownictwa oraz procedury zapewniające szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem informacji.	L	N	Procedura reakcji na incydenty obecnie jest elementem wsparcia realizowanym w ramach serwisu. Wymagane regularne przeglądy poprawności działania pozwalają na wykrycie niekorzystnych zdarzeń i podjęcie odpowiednich działań. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
16.1.2.	Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji	Zdarzenia związane z bezpieczeństwem informacji należy zgłaszać odpowiednimi kanałami zarządczymi tak szybko, jak tylko to jest możliwe.	L	N	Zgłaszanie zdarzeń jest elementem usługi serwisu/konserwacji. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
16.1.3.	Zgłaszanie słabości związanych z bezpieczeństwem informacji	Należy zobowiązać pracowników oraz kontrahentów korzystających z systemów i usług informacyjnych organizacji do odnotowania i zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji w systemach lub usługach.	L	N	Jak wyżej.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
16.1.4.	Ocena i podejmowanie decyzji w sprawie zdarzeń związanych z bezpieczeństwem informacji	Zdarzenia związane z bezpieczeństwem informacji należy ocenić i podjąć decyzję w sprawie zakwalifikowania ich jako incydentów związanych z bezpieczeństwem informacji.	F	N	Producent/dostawca w ramach wsparcia/serwisu przygotowuje właściwe zmiany i aktualizacje zgodnie z procedurami opisanymi w przepisach. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
16.1.5.	Reagowanie na incydenty związane z bezpieczeństwem informacji	Reakcja na incydenty związane z bezpieczeństwem informacji powinna być zgodna z udokumentowanymi procedurami.	L	N	Jak wyżej.
16.1.6.	Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji	Wiedzę zdobytą podczas analizy i rozwiązywania incydentów związanych z bezpieczeństwem informacji należy wykorzystać do zredukowania prawdopodobieństwa wystąpienia lub skutków przyszłych incydentów.	F	N	Jak wyżej.
16.1.7.	Gromadzenie materiału dowodowego	Organizacja powinna określić i stosować procedury identyfikacji, gromadzenia, pozyskiwania i utrwalania informacji, które mogą stanowić materiał dowodowy.	F	N	Konstrukcyjnie (pamięć fiskalna, pamięć chroniona) urządzenia są przygotowane do gromadzenia materiału dowodowego. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
17.	**Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania**		1	0	
17.1.	Ciągłość bezpieczeństwa informacji Cel: Zaleca się uwzględnienie ciągłości bezpieczeństwa informacji w systemach zarządzania ciągłością działania organizacji.		1	0	W przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania istnieje istotne ryzyko nieuwzględnienia zapewnienia ciągłości bezpieczeństwa informacji w zarządzaniu ciągłością działania.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
17.1.1.	Planowanie ciągłości bezpieczeństwa informacji	Organizacja powinna określić wymagania dotyczące bezpieczeństwa informacji i ciągłości zarządzania bezpieczeństwem informacji w niekorzystnych sytuacjach np. w czasie kryzysu lub katastrofy.	F	N	Obecne przepisy regulują kwestie ciągłości działania i określają skuteczność zasilania akumulatorowego w liczbie operacji. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
17.1.2.	Wdrożenie ciągłości bezpieczeństwa informacji	Organizacja powinna ustanowić, udokumentować, wdrożyć i utrzymywać procesy, procedury i zabezpieczenia dla zapewnienia w niekorzystnej sytuacji wymaganego poziomu ciągłości bezpieczeństwa informacji.	F	N	Element ciągłości działania operacyjnego na akumulatorze podlega testom certyfikacyjnym prowadzonym przez GUM. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
17.1.3.	Weryfikowanie, przegląd i ocena ciągłości bezpieczeństwa informacji	Organizacja powinna weryfikować ustanowione i wdrożone zabezpieczenia ciągłości bezpieczeństwa informacji w regularnych odstępach czasu celem zapewnienia ich aktualności i skuteczności w niekorzystnych sytuacjach.	F	N	Element ciągłości działania operacyjnego na akumulatorze podlega testom w ramach obowiązkowych, regularnych prac konserwacyjnych. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
17.2.	Nadmiarowość Cel: Zapewnić dostępność środków przetwarzania informacji.		1	1	Wyłączenie - zabezpieczenie nie ma zastosowania.
17.2.1.	Dostępność środków przetwarzania informacji	Środki przetwarzania informacji należy wdrażać z nadmiarem wystarczającym do spełnienia wymagań dostępności.	X	X	Wyłączenie - zabezpieczenie nie ma zastosowania.
18.	**Zgodność**		**1**	**0**	
18.1.	Zgodność z wymaganiami prawnymi i umownymi Cel: Unikać naruszenia zobowiązań prawnych, regulacyjnych lub umownych związanych z bezpieczeństwem informacji oraz innych wymagań dotyczących bezpieczeństwa.		1	0	Istnieje ryzyko braku zgodności z wymaganiami prawnymi w przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania.

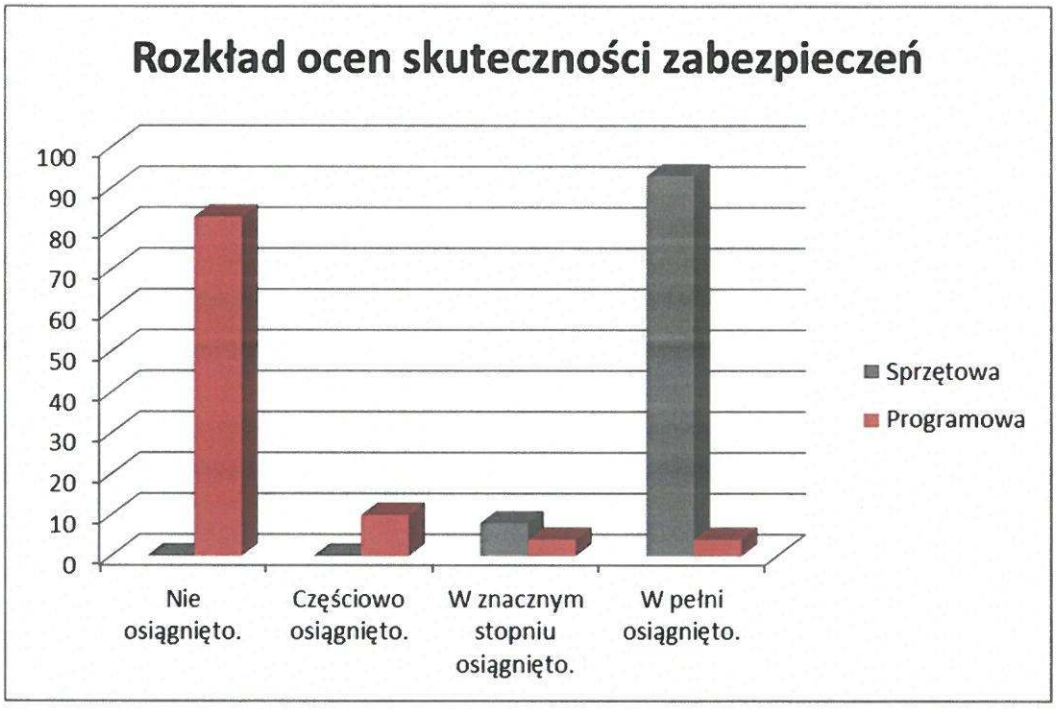
Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
18.1.1.	Określenie stosownych wymagań prawnych i umownych	Wszystkie istotne wymagania prawne, regulacyjne, umowne oraz podejście organizacji do ich przestrzegania należy zidentyfikować, udokumentować i aktualizować dla każdego systemu informacyjnego oraz całości organizacji.	F	P	Propozycje zawarte w **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania są niekompletne, gdyż nie regulują wymagań wobec systemu jako całości (są fragmentaryczne) i pomijają wiele aspektów mających wpływ na bezpieczeństwo informacji.
18.1.2.	Prawa własności intelektualnej	Należy wdrożyć odpowiednie procedury zapewniające zgodność z wymaganiami prawnymi, regulacyjnymi i umownymi, związanymi z prawami własności intelektualnej i użytkowaniem prawnie zastrzeżonego oprogramowania.	F	N	Obecnie prowadzony system dystrybucji zapewnia ochronę praw własności intelektualnej. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.
18.1.3.	Ochrona zapisów	Zapisy należy chronić przed utratą, zniszczeniem, fałszowaniem, nieuprawnionym dostępem i nieuprawnionym opublikowaniem, stosownie do wymagań prawnych, regulacyjnych, umownych i biznesowych.	F	N	Przyjęty obecnie model kasy rejestrującej zapewnia właściwą ochronę zapisów. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie. Sam fakt przesyłania danych nie zapewnia ochrony wszystkich zapisów.
18.1.4.	Prywatność i ochrona danych identyfikujących osobę	Należy zapewnić prywatność i ochronę danych identyfikujących osobę stosownie do odpowiednich przepisów prawa i regulacji.	X	X	Wyłączenie - zabezpieczenie nie ma zastosowania.

Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
18.1.5.	Regulacje dotyczące zabezpieczeń kryptograficznych	Zabezpieczenia kryptograficzne należy stosować zgodnie z odpowiednimi umowami, przepisami i regulacjami.	F	L	Przepisy określają wymagania w zakresie zabezpieczeń kryptograficznych. Okres ważności certyfikatu producenta oprogramowania w **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania wydaje się zbyt długi (10 lat). Ponadto nie określono wymagań w zakresie wydania ani metod kontroli wydawania przez ten podmiot certyfikatów indywidualnych dla każdej instalacji kasy. Istniejące podatności w platformie systemowej mogą umożliwić klonowanie tych certyfikatów.
18.2.	Przeglądy bezpieczeństwa informacji Cel: Zapewnić zgodne z politykami organizacji i procedurami wdrożenie i stosowanie zasad bezpieczeństwa informacji.		1	0	Istnieje istotne ryzyko braku zgodności stosowanych zasad bezpieczeństwa z najlepszymi praktykami w przypadku **Projektu** dotyczącego wprowadzenia kas rejestrujących mających postać oprogramowania.
18.2.1.	Niezależny przegląd bezpieczeństwa informacji	Podejście organizacji do zarządzania bezpieczeństwem informacji oraz jego wdrożenie (tzn. cele stosowania zabezpieczeń, zabezpieczenia, polityki, procesy i procedury dotyczące bezpieczeństwa informacji) należy poddawać niezależnemu przeglądowi w zaplanowanych odstępach czasu lub wtedy, gdy nastąpią istotne zmiany.	F	N	Niezależny przegląd bezpieczeństwa informacji jest prowadzony regularnie w oparciu o bieżące przepisy w trakcie regularnych procedur konserwacyjnych. W **Projekcie** dotyczącym wprowadzenia kas rejestrujących mających postać oprogramowania nie zidentyfikowano wymagań w tym zakresie.

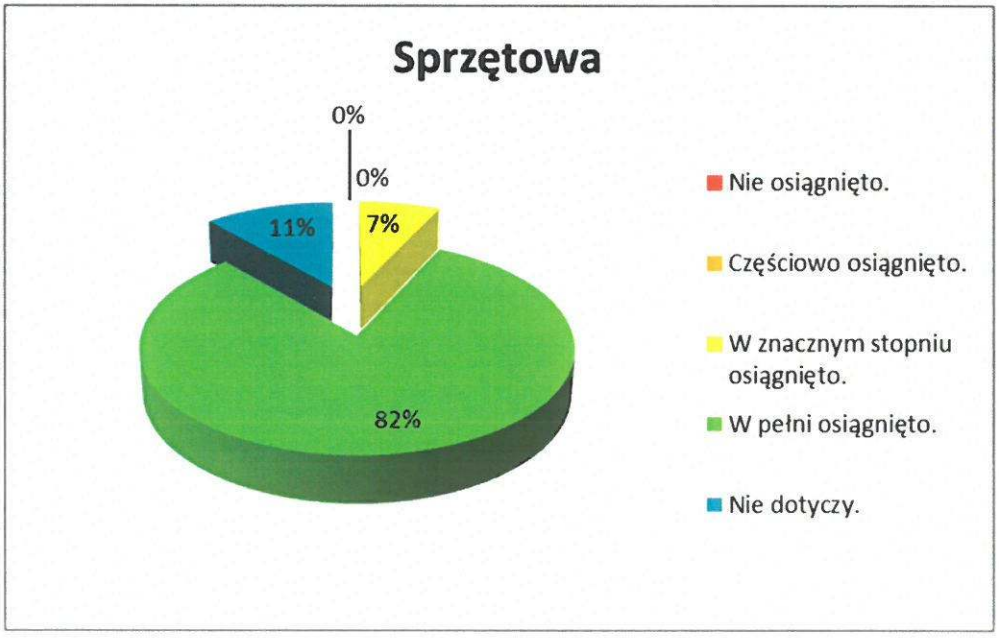
Nr	Nazwa	Zabezpieczenie	Sprzętowa	Programowa	Spostrzeżenia
18.2.2.	Zgodność z politykami bezpieczeństwa i standardami	Kierownicy powinni regularnie dokonywać przeglądu zgodności przetwarzania informacji i procedur z odpowiednimi politykami bezpieczeństwa, standardami i innymi wymaganiami dotyczącymi bezpieczeństwa, w zakresie przydzielonej im odpowiedzialności.	F	N	Jak wyżej.
18.2.3.	Sprawdzanie zgodności technicznej	Należy regularnie przeglądać systemy informacyjne celem sprawdzenia ich zgodności z politykami bezpieczeństwa informacji i standardami obowiązującymi w organizacji.	F	N	Jak wyżej.

5. Analiza, uwagi i spostrzeżenia

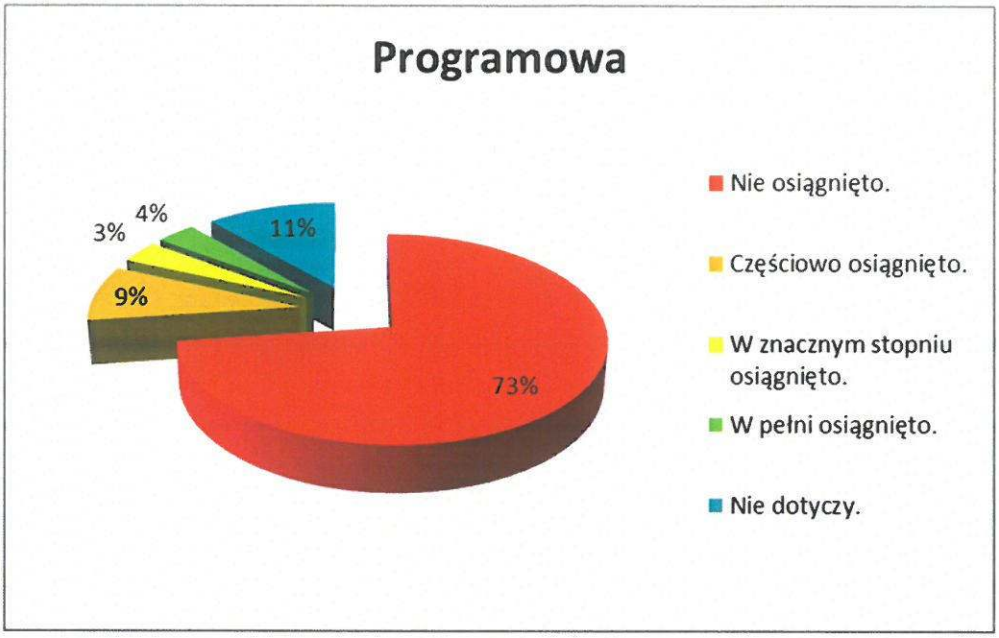
Z przeprowadzonego w poprzednim rozdziale badania wynika, że przedstawiony projekt Rozporządzenia pomija wiele bardzo istotnych aspektów ryzyka. Jest to doskonale widoczne na poniższych diagramach, gdzie w przypadku wersji wynikającej z **Projektu** nazywanej wersją **Programową** dominują oceny **nie osiągnięto**, które wskazują na najwyższy poziom ryzyka (niepewności w obszarze chronionym przez wymagane zabezpieczenie).



Rysunek 4 Rozkład ocen skuteczności zabezpieczeń.



Rysunek 5 Rozkład poziomów dojrzałości zabezpieczeń dla kasy rejestrującej sprzętowej.



Rysunek 6 Rozkład poziomów dojrzałości zabezpieczeń dla kasy rejestrującej w formie oprogramowania.

Podstawowe różnice w ocenie ryzyka wynikają z faktu, że na system informacyjny składa się nie tylko oprogramowanie. Oprogramowanie do działania wymaga właściwego sprzętu, usług, ludzi i procedur. Dotyczy to zarówno rozwiązań chmurowych (nawet reklamowanych jako *serverless*[2]), jak i opartych o fizyczne centra przetwarzania danych.

Architektura systemów informacyjnych ma budowę warstwową[3]. Oznacza ona, że komunikacja zachodzi tylko pomiędzy sąsiadującymi warstwami, niezależnie od tego czy jest to sieć teleinformatyczna, czy system operacyjny. Ma to tę zaletę, że niezależnie od fizycznej budowy sieci, czy komputera pod warunkiem, że będzie to ten sam protokół komunikacyjny i/lub system operacyjny, będziemy w stanie uruchomić to samo oprogramowanie, a warstwy pośrednie dostarczone przez operatora sieci lub dostawcę sprzętu. Jednak każdy medal ma dwie strony. Oprogramowanie nie będzie w stanie rozróżnić szczegółów technicznych rozwiązania, na którym pracuje.

Funkcjonujące obecnie rozwiązanie kas rejestrujących ewoluowało uwzględniając zmiany w środowisku i obecnie można uznać je za rozwiązanie dojrzałe. Przede wszystkim bazuje ono na certyfikacji rozwiązań kompletnych, zamkniętych i funkcjonujących. Certyfikacja dokonywana jest przez osoby posiadające odpowiednią wiedzę i doświadczenie (GUM). Każda próba ingerencji w rozwiązanie jest łatwa do wykrycia przez osobę nie dysponującą laboratorium badawczym i wiedzą specjalistyczną z zakresu architektury systemów komputerowych, administrowania systemami operacyjnymi, czy badaniem podatności nazywanym często niepoprawnie testami penetracyjnymi. Wprowadzając tak daleko idącą zmianę należałoby postawić co najmniej dwa kluczowe pytania. Czy taką wiedzę specjalistyczną posiadają pracownicy KAS udający się na kontrolę podatnika? Czy taką wiedzą specjalistyczną dysponuje podatnik?

2 **https://serverlesspolska.pl/2019/11/21/Nie-bezpieczenstwo-w-Serverless/**
3 Model OSI **https://pl.wikipedia.org/wiki/Model_OSI** sieć Internet **https://pl.wikipedia.org/wiki/Model_TCP/IP** czy system operacyjny **https://pl.wikipedia.org/wiki/System_operacyjny**

Odpowiedź na to pytanie brzmi nie. To znaczy, że zapisany w rozporządzeniu zbiór obowiązków (w szczególności w § 12) nie może być spełniony (*Impossibilium nulla obligatio est* – Zobowiązanie do (świadczenia) niemożliwego jest nieważne).

Systemy operacyjne w rozwiązaniach konsumenckich, takich jak tablety czy telefony z systemem Android nie były projektowane jako „środowisko bezpieczne". Nie zapewniają domyślnie odpowiedniej separacji uprawnień. Okres wsparcia producenta i poprawiania wykrywanych luk i błędów jest krótki, a reakcja producenta w kwestii przygotowania poprawek oprogramowania systemowego, szczególnie w przypadku wielu modeli „z niskiej półki" (a wiec tanich na tyle aby być konkurencją dla kas rejestrujących), jest co najmniej nieakceptowalna. Oznacza to, że urządzenia takie nie zapewnią właściwego środowiska do pracy oprogramowania pełniącego funkcję kasy rejestrującej.

Urządzenia te umożliwiają instalację różnego oprogramowania, które może ingerować w inne oprogramowanie. Może to być zarówno działanie przypadkowe, jak również celowe. Bez odpowiedniego przygotowania osób kontrolujących (pracowników KAS) stwierdzenie tego faktu nie jest możliwe a koszty analiz specjalistycznych (ang. *forensic analysis*) są kosztowne i długotrwałe.

6. Podsumowanie

Na podstawie przeprowadzonej analizy stwierdzono, że przedstawiony projekt Rozporządzenia pomija wiele bardzo istotnych aspektów ryzyka, które zostały całkowicie pominięte w Ocenie Skutków Regulacji. Ocena Skutków Regulacji nie odnosi się do wymagań bezpieczeństwa informacji, a w szczególności do norm wskazanych bezpośrednio w ustawach o **KSC** i **KRI**.

Stosowanie kas rejestrujących w formie oprogramowania jest co do zasady kierunkiem dobrym, gdyż upraszcza i łagodzi wymagania wobec przedsiębiorców. Jednakże decyzja dotycząca przyjęcia tego rozwiązania wymaga uwzględnienia ryzyka dla całości rozwiązania. To znaczy, że może być stosowane tam, gdzie istnieje rękojmia należytego nadzoru nad wszystkim składnikami systemu. Zbiór wymagań w tym zakresie można sformułować następująco:

1) Oprogramowanie powinno podlegać certyfikacji. Producent oprogramowania powinien móc uzyskać certyfikat cyfrowy do podpisywania swojego produktu tylko i wyłącznie po spełnieniu wymagań w zakresie procesu wytwórczego oprogramowania.
2) Powinny być określone wymagania dla środowiska w jakim to oprogramowanie ma być uruchamiane, a w szczególności wymagania dotyczące bezpiecznej konfiguracji (ang. *hardening*).
3) Powinny być określone wymagania dotyczące modelu utrzymania bazujące na normie PN-EN ISO/IEC 27001 oraz PN-EN ISO 22301, a w szczególności posiadania ważnych akredytowanych certyfikatów systemów zarządzania w tym zakresie.

Wprowadzenie kas rejestrujące mających postać oprogramowania powinno zostać poprzedzone szczegółową analizą ryzyka z uwzględnieniem obowiązujących wymagań prawnych oraz norm i standardów międzynarodowych.

Opinię opracował Zespół pod kierownictwem rzeczoznawcy Polskiego Towarzystwa Informatycznego Pawła Heniga.

POLSKIE TOWARZYSTWO INFORMATYCZNE
PTI
Paweł Henig
RZECZOZNAWCA NR 092

Paweł Henig
Kierownik Zespołu wykonawców

Tomasz Szatkowski
Dyrektor Izby Rzeczoznawców PTI

Warszawa, dnia: 13 grudnia 2019 roku.