Nazwa projektu Ustawa o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw **Ministerstwo wiodące i ministerstwa współpracujące** Dyrektor Rządowego Centrum Bezpieczeństwa **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan Zbigniew Muszyński, dyrektor Rządowego Centrum Bezpieczeństwa **Kontakt do opiekuna merytorycznego projektu** (pkt I rozwiązań zawartych w projekcie) Pan Karol Stec, Szef Wydziału Oceny Ryzyka i Planowania tel. kom 532-451-765, e-mail: karol.stec@rcb.gov.pl (pkt II rozwiązań zawartych w projekcie) Pan Witold Skomra, Doradca w Rządowym Centrum Bezpieczeństwa tel. kom. 785-700-176, e-mail: witold.skomra@rcb.gov.pl	**Data sporządzenia** 03.07.2024 r. **Źródło:** Upoważnienie Prezesa Rady Ministrów Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, z późn. zm.) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022 r. str. 164), **Nr w wykazie prac: UC47**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

I. Wdrożenie rozwiązań zapewniających podstaw zarządzania ryzykiem, z uwzględnieniem postanowień Decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, L 250 z 04.10.2018, str. 1 oraz L 77A z 20.03.2019, str. 1), zwanej dalej „UMOL".

Posiadanie planów zarządzania ryzykiem jest o tyle istotne, iż są one niezbędne do spełnienia tzw. warunkowości ex ante w perspektywie finansowej UE na lata 2021-2027, co ma przełożenie na możliwość pozyskiwania środków finansowych w ramach polityki spójności z Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności oraz Europejskiego Funduszu Morskiego i Rybackiego.

Opracowanie dokumentów planistycznych w obszarze zarządzania ryzykiem jest bowiem bezpośrednio powiązane z jednym z warunków podstawowych perspektywy finansowej, który mówi o „osiągnięciu skutecznych ram zarządzania ryzykiem". Wskazuje się wprost na konieczność opracowania planu zarządzania ryzykiem na szczeblu krajowym lub regionalnym, powiązanego ze strategiami adaptacji do zmian klimatu. Ponadto państwa członkowskie opracowują oceny ryzyka na szczeblu krajowym lub niższym oraz udostępniają Komisji Europejskiej tzw. streszczenie istotnych elementów tych ocen.

Obowiązujące obecnie w tym obszarze regulacje ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym nie pozwalają w pełni odzwierciedlać w planach zarządzania kryzysowego kwestii dotyczących zarządzania ryzykiem. Istnieje zatem konieczność opracowywania planów zarządzania ryzykiem, na szczeblu krajowym lub odpowiednio niższym, wskazanie podmiotów odpowiedzialnych za ich opracowanie, zakresu merytorycznego takiego planu oraz określenie cyklu planowania.

Konieczne jest tym samym modyfikacja dotychczasowych rozwiązań w kierunku zapewnienia podstaw prawnych i organizacyjnych dotyczących kwestii zarządzania ryzykiem, co znajdzie odzwierciedlenie w projekcie w rozwiązaniach dotyczących dokumentów strategicznych w zakresie oceny ryzyka oraz treści planów zarządzania kryzysowego. Nowe regulacje pozwolą również na efektywne przekazywanie dokumentów o charakterze sprawozdawczym Komisji Europejskiej, m.in. „Streszczenia istotnych elementów krajowej oceny ryzyka" oraz „Streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem".

II. Wdrożenie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022 r. str. 164), zwaną dalej „dyrektywą CER".
Zapewnienie ciągłości świadczenia usług kluczowych realizowanych w sektorach lub podsektorach wskazanych w dyrektywie CER.
Identyfikacja usług kluczowych świadczonych przez operatorów infrastruktury krytycznej z uwzględnieniem

potencjalnych skutków zakłócenia zarówno w odniesieniu do funkcjonowania państwa jak i społeczeństwa. Minimalizacja skutków zakłócenia poprzez wprowadzenie procesów oceny i zarządzania ryzykiem. Uwzględnienie zadań związanych z ochroną usług kluczowych i infrastruktury krytycznej o szczególnym znaczeniu europejskim. Modyfikacja obecnych rozwiązań dotyczących infrastruktury krytycznej jako niezbędnych elementów świadczenia usług kluczowych.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

I. W zakresie kwestii zarządzania ryzykiem, z uwzględnieniem postanowień UMOL przewiduje się wdrożenie zintegrowanego podejścia do zarządzania ryzykiem, obejmującego cały cykl zarządzania, od oceny ryzyka poprzez przygotowanie planów zarządzania nim oraz wdrażanie środków zapobiegawczych i zapewniających gotowość do ich użycia.

Przewiduje się opracowanie na szczeblu centralnym dokumentu rządowego, tzw. Krajowej Oceny Ryzyka, który zastąpi obecnie funkcjonujący Raport o zagrożeniach bezpieczeństwa narodowego. Dotychczasowe doświadczenia wykazują, że Raport o zagrożeniach bezpieczeństwa narodowego jest dokumentem nadmiernie obszernym, mającym charakter quasi cyklicznej oceny zidentyfikowanych zagrożeń, a jednocześnie nie przekładającym się na procesy planistyczne dotyczące zarządzania ryzykiem.

Krajowa Ocena Ryzyka będzie funkcjonalnym dokumentem zawierającym zidentyfikowane zagrożenia o różnym charakterze (naturalne, techniczne, związane z konfliktem zbrojnym w tym hybrydowe, o charakterze terrorystycznym, z obszaru cyberbezpieczeństwa, itp.) oraz ocenę ryzyk wynikających z tych zagrożeń, pozwalającą określić cele strategiczne i priorytety na rzecz ich ograniczania. Istotne jest bowiem zrozumienie, że dopiero prawidłowo przeprowadzona ocena ryzyka, identyfikuje zagrożenia i obszary, w których konieczne jest podjęcie działań, w tym zwiększenie nakładów finansowych na realizację przedsięwzięć ograniczających.

Krajowa Ocena Ryzyka – w obszarze planowania cywilnego – wykorzystywana będzie wykorzystywana na potrzeby opracowania Krajowego Planu Zarządzania Kryzysowego oraz planów zarządzania kryzysowego ministrów, kierowników urzędów centralnych, wojewodów, jak również planów zarządzania kryzysowego na szczeblu powiatu oraz gminy. Każdy z planów będzie zawierał cześć obejmującą zarządzanie ryzykiem (działania w zakresie zapobiegania sytuacji kryzysowej oraz przygotowywania do jej wystąpienia) oraz cześć dotyczącą reagowania kryzysowego (działania w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków).

W przypadku planów na szczeblu gminnym – ujęcie w planie zarządzania kryzysowego kwestii dotyczących zarządzania ryzykiem będzie fakultatywne.

Konieczne będzie dostosowanie terminologii do regulacji unijnych, co stworzy efektywne narzędzia do prowadzenia oceny ryzyka i zarządzania nim. Jednocześnie zostaną ujednolicone terminy cyklów planistycznych krajowych z unijnymi, gdyż obowiązujące przepisy krajowe przewidują cykl 2-letni, podczas gdy unijne regulacje wskazują na 3-letnie cykle planistyczne. Nowy cykl planistyczny będzie obejmował 3 lata.

Dodatkowo przewiduje się, że Krajowa Ocena Ryzyka oraz Krajowy Plan Zarządzania Kryzysowego będą punktami odniesienia do opracowania dokumentów udostępnianych Komisji Europejskiej w ramach realizacji postanowień UMOL, tj. odpowiednio:
1) streszczenia istotnych elementów krajowej oceny ryzyka;
2) streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem.

II. Wdrożenie rozwiązań zawartych w dyrektywie CER nie może odbyć się bez redefiniowania regulacji dotyczących infrastruktury krytycznej, która jest niezbędna do świadczenia usług kluczowych przez podmioty krytyczne, o których traktuje CER. W szczególności należy doprowadzić do niezakłóconego „przejścia" z dotychczasowych systemów infrastruktury krytycznej na sektory i podsektory, o których mówi dyrektywa. Ponadto, biorąc pod uwagę że dyrektywa stanowi jedynie minimum harmonizacyjne, projekt zakłada nie tylko utrzymanie dotychczasowego poziomu ochrony infrastruktury krytycznej, ale również wprowadzenie dodatkowych mechanizmów zapewniających jej ochronę, nawet już na etapie jej projektowania lub budowy.
Projektowane rozwiązania mają na celu wzmocnienie mechanizmów ochrony infrastruktury krytycznej, biorąc pod uwagę, iż stanowi ona rdzeń świadczenia usług niezbędnych dla funkcjonowania państwa oraz jego obywateli. Wynikają one również z analizy przebiegu wojny w Ukrainie i pojawiających się działań o charakterze sabotażowym i hybrydowym.

Infrastruktura krytyczna
Przewiduje się nowe kryteria umożliwiające identyfikację obiektów, instalacji oraz urządzeń jako infrastruktury krytycznej, a tym samym wyłaniania operatorów infrastruktury krytycznej (właściciel lub posiadacz takiej infrastruktury). Jednocześnie z kryteriami zostanie wskazany mechanizm identyfikacji infrastruktury krytycznej przez ministrów kierującymi działami administracji rządowej, wojewodów oraz przez inne podmioty, w zakresie ich właściwości. Ponadto zostaną wskazane ramy współpracy na linii administracja publiczna – przedsiębiorcy, będący operatorami infrastruktury krytycznej.

W celu zapewnienia właściwego poziomu ochrony infrastruktury krytycznej przewiduje się wprowadzenie minimalnych standardów w obszarach bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz zapewnienia planów ciągłości działania i odtwarzania.

Do obowiązków operatorów infrastruktury krytycznej będzie należało opracowanie i wdrożenie rozwiązań w zakresie infrastruktury krytycznej uwzględniającej minimalne standardy. Dodatkowo operator będzie zobowiązany do opracowania i prowadzenia dokumentacji odzwierciedlającej wdrożone rozwiązania, która to dokumentacja zastąpi obecne plany ochrony infrastruktury krytycznej.
Przewiduje się wprowadzenie instytucji koordynatora do spraw ochrony infrastruktury krytycznej u operatorów infrastruktury krytycznej. Operatorzy infrastruktury krytycznej będą obowiązani wyznaczać osoby koordynujące działania na linii operator – organy administracji publicznej, co jest analogią do obecnie wyznaczonych tzw. osób kontaktowych, funkcjonujących u operatorów infrastruktury krytycznej.
Zmiana ta nie generuje dodatkowych kosztów dla operatorów IK, natomiast wprowadza efektywnie działające narzędzie systemowe w zakresie organizacji ochrony infrastruktury krytycznej. Dokonuje instytucjonalizacji osoby do utrzymywania kontaktów, zastępując ją funkcją „koordynatora ochrony infrastruktury krytycznej".
Koordynatorowi zostaną przyznane stosowne kompetencje – będzie on realizował działania przypisane ustawowo operatorowi i w jego imieniu.

Elementem „weryfikującym" poziom ochrony infrastruktury krytycznej oraz stopień wdrożenia rozwiązań w tym zakresie, będą raporty operatorów zawierające w szczególności informacje dotyczące funkcjonowania ochrony infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz zapewnienia planów ciągłości działania i odtwarzania. Raportowanie o stanie infrastruktury krytycznej w obowiązującym stanie prawnym dotyczy tylko systemu zaopatrzenia w energię, surowce energetyczne i paliwa. Dotychczas raporty te w powyżej wskazanym systemie sporządzane były z częstotliwością raz na kwartał. W odniesieniu do pozostałych systemów obowiązywało raportowanie doraźne.

Projektowane rozwiązania przewidują obowiązek okresowego raportowania przez wszystkich operatorów infrastruktury krytycznej, a cykl raportowania zostanie ujednolicony i będzie wynosił 12 miesięcy. W odniesieniu do przypadków wystąpienia incydentu naruszającego bezpieczeństwo infrastruktury krytycznej - operator zobowiązany będzie do doraźnego sporządzania raportów w tym zakresie.

Raport o stanie ochrony infrastruktury krytycznej sporządzany będzie m.in. z uwzględnieniem rozwiązań wdrożonych przez operatora, informacji zawartych w dokumentacji ochrony infrastruktury krytycznej, możliwości wystąpienia zidentyfikowanych ryzyk, incydentów oraz zdarzeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, wyników przeprowadzonych kontroli i audytów odnoszących się do zabezpieczeń infrastruktury krytycznej.
Z tytułu jego sporządzania operatorzy nie będą ponosić dodatkowych kosztów.

Usługi kluczowe
Rada Ministrów określi w drodze rozporządzenia wykaz usług kluczowych w poszczególnych sektorach lub podsektorach, wskazując jednocześnie kategorie podmiotów mogących świadczyć usługi oraz tzw. „progi istotności" skutku zakłócającego daną usługę.
Usługi kluczowe, co do zasady, będą realizowane przez operatorów infrastruktury krytycznej, za pomocą posiadanej przez nich infrastruktury. Niemniej jednak aby operator infrastruktury krytycznej uzyskał status podmiotu krytycznego – konieczne jest przeprowadzenie jego identyfikacji w oparciu o ww. rozporządzenie Rady Ministrów.

Strategia Odporności Podmiotów Krytycznych
W celu jak najlepszego doboru działań zmierzających do identyfikacji podmiotów krytycznych, zbudowania ich odporności i zapewnienia niezakłóconego świadczenia usług kluczowych – opracowany zostanie, na szczeblu krajowym, dokument o charakterze strategicznym. Strategia określi cele i priorytety w zakresie zapewnienia niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne i operatorów infrastruktury krytycznej jak również określi wszelkie niezbędne zakresy działań oraz formy działań służące osiąganiu tych celów. Strategia wskaże również podmioty właściwe do realizacji postanowień strategii oraz określi ich role.

Podmioty krytyczne
Wzorując się na dyrektywie CER – przyjmuje się, że podmiotem krytycznym może być operator infrastruktury krytycznej, prowadzący działalność na terytorium RP, który świadczy co najmniej jedną usługę kluczową a incydent miałby istotny skutek zakłócający jej świadczenie.
Podmioty krytyczne będą identyfikowane przez wskazane ustawą organy do spraw podmiotów krytycznych i ujmowane w wykazach podmiotów krytycznych, prowadzonych przez te organy, zgodnie z ich właściwością.

Podmiot krytyczny będzie obowiązany do:

1) prowadzenia systematycznej oceny ryzyka świadczonej usługi kluczowej;
2) wdrożenia odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi (w tym infrastruktury krytycznej, za pomocą której świadczona jest usługa kluczowa), z uwzględnieniem polskich norm;
3) zapewnienia obsługi incydentów mających wpływ na świadczenie usługi kluczowej, w tym informowania o incydentach właściwych organów do spraw podmiotów krytycznych;
4) informowanie właściwych organów zarządzania kryzysowego o incydentach mających istotny wpływ na świadczenie usługi kluczowej, w przypadku gdy może to doprowadzić do sytuacji kryzysowej;
5) zapewnienia przeprowadzenia cyklicznych audytów wdrożonych rozwiązań, o których mowa w pkt 2;
6) zapewnienia udziału struktur organizacyjnych lub pracowników w szkoleniach i ćwiczeniach, w tym ćwiczeniach z zakresu obrony cywilnej, ochrony ludności, zarządzania kryzysowego oraz obronnych;
7) wyznaczenia tzw. osób odpowiedzialnych za utrzymanie kontaktów z właściwymi organami do spraw podmiotów krytycznych oraz zapewnienie im organizacyjnych warunków realizacji funkcji.

Zgodnie z dyrektywą CER projektowane przepisy określą również sposób identyfikacji i wyznaczania tzw. podmiotu krytycznego o szczególnym znaczeniu europejskim oraz wskażą obowiązki z tym związane.

Organy do spraw podmiotów krytycznych

Projektowana regulacja wskaże organy do spraw podmiotów krytycznych w poszczególnych sektorach i podsektorach.
Do podstawowych zadań organu należeć będzie:
1) prowadzenie bieżącej analizy podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za podmiot krytyczny oraz ujmowania ich w wykazie;
2) prowadzenie bieżącej analizy podmiotów krytycznych w danym sektorze lub podsektorze pod kątem niespełniania warunków kwalifikujących dany podmiot jako podmiot krytyczny oraz wykreślanie ich z wykazu;
3) monitorowanie stosowania przepisów ustawy przez podmioty krytyczne;
4) prowadzanie kontroli podmiotów krytycznych;
5) nakładanie kar;
6) uczestniczenie w planowaniu, organizowaniu ćwiczeń podmiotów krytycznych oraz w razie potrzeby udział w tych ćwiczeniach;
7) prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania wiadomości w zakresie bezpieczeństwa usług kluczowych przez podmioty krytyczne.

Rządowe Centrum Bezpieczeństwa

Mając na względzie dotychczasowa praktykę w zakresie koordynacji zadań na szczeblu krajowym w zakresie ochrony infrastruktury krytycznej – przewiduje się, iż do zadań RCB należeć będzie:
1) monitorowanie wdrażania Strategii;
2) wykonywanie – z upoważnienia Prezesa Rady Ministrów – obsługi czynności Prezesa Rady Ministrów jako organu do spraw podmiotów krytycznych w sektorze administracja publiczna;
3) opracowywanie rocznych sprawozdań dotyczących tzw. incydentów istotnych zgłaszanych przez podmioty krytyczne, mających wpływ na ciągłość świadczonych przez nich usług kluczowych;
4) prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania świadomości w zakresie bezpieczeństwa świadczenia usług kluczowych przez podmioty krytyczne;
5) gromadzenie informacji o incydentach istotnych, które zostały przekazane przez inne państwa członkowskie Unii Europejskiej;
6) udostępnianie informacji i dobrych praktyk związanych ze zgłaszaniem incydentów istotnych przez podmioty krytyczne, uzyskane z tzw. Grupy do spraw Odporności Podmiotów Krytycznych;
7) prowadzenie tzw. Pojedynczego Punktu Kontaktowego, do którego zadań należeć m.in. będzie:
    a) odbieranie zgłoszeń incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej,
    b) przekazywanie zgłoszenia incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej;
    c) zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie do spraw Podmiotów Krytycznych,
    d) zapewnienie współpracy z Komisją Europejską w obszarze bezpieczeństwa świadczenia usług kluczowych,
    e) koordynacja współpracy między organami do spraw podmiotów krytycznych i organami administracji publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej,
    f) zapewnienie wymiany informacji na potrzeby Grupy do spraw Odporności Podmiotów Krytycznych oraz organami do spraw podmiotów krytycznych.

Nadzór i kontrola podmiotów krytycznych

Przewiduje się, iż nadzór w zakresie stosowania przepisów ustawy sprawują organy do spraw podmiotów krytycznych w zakresie:

1) spełniania przez podmioty krytyczne wymogów bezpieczeństwa dotyczących świadczenia usług kluczowych;
2) wykonywania przez podmioty krytyczne obowiązków dotyczących przeciwdziałania zagrożeniom dla świadczonych usług kluczowych i zgłaszania incydentów istotnych.

W ramach nadzoru organ do spraw podmiotów krytycznych:

1) prowadzi kontrole podmiotów krytycznych;
2) przeprowadza lub zleca audyt rozwiązań dotyczących bezpieczeństwa świadczenia usługi kluczowej;
3) nakłada kary pieniężne na podmioty krytyczne.

Projektowane rozwiązania przewidują, iż do kontroli realizowanej wobec podmiotów:

1) będących przedsiębiorcami stosuje się przepisy ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców;
2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej.

Przepisy o karach pieniężnych

Przepisy w tym zakresie wskażą – w zgodzie z dyrektywą CER – zamknięty katalog kar nakładanych na podmioty krytyczne za niestosowanie się do przepisów ustawy oraz sposób zagospodarowania wpływów z tytułu tych kar.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Obowiązek opracowania planów zarządzania ryzykiem jest wdrażany w innych krajach UE, co wynika z postanowienia Decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności. Brak jest danych dotyczących wdrożonych rozwiązań w innych państwach w tym obszarze.

W przypadku ochrony usług kluczowych – koncepcja zawarta w dyrektywie CER jest rozwiązaniem odmiennym od stosowanego dotychczas w Unii Europejskiej tzw. „podejścia obiektowego". W efekcie wszystkie kraje UE stają przed problemem zaimplementowania rozwiązań, które dotychczas nie było stosowane. Brak tym samym rozwiązań, które mogłyby być przeanalizowane na potrzeby opracowania projektu ustawy.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Planowanie cywilne – wdrożenie postanowień UMOL			
Ministrowie kierujący działami administracji rządowej	19		Opracowanie wkładów do Krajowej Oceny Ryzyka oraz Krajowego Planu Zarządzania Kryzysowego. Opracowanie planów zarządzania kryzysowego uwzględniających zarządzanie ryzykiem.
Kierownicy urzędów centralnych	40		Opracowanie wkładów do Krajowej Oceny Ryzyka oraz Krajowego Planu Zarządzania Kryzysowego. Opracowanie planów zarządzania kryzysowego uwzględniających zarządzanie ryzykiem.
Wojewodowie	16		Opracowanie wkładów do Krajowej Oceny Ryzyka oraz Krajowego Planu Zarządzania Kryzysowego. Opracowanie planów zarządzania kryzysowego uwzględniających zarządzanie ryzykiem.
Rządowe Centrum Bezpieczeństwa	1		Opracowanie Krajowej Oceny Ryzyka, opracowanie

			Krajowego Planu Zarządzania Kryzysowego
Powiaty	314		Opracowanie planów zarządzania kryzysowego uwzględniających zarządzanie ryzykiem.
Gminy	2 477		Opracowanie planów zarządzania kryzysowego z możliwością uwzględnienia zarządzania ryzykiem.
Implementacja dyrektywy CER			
Operatorzy infrastruktury krytycznej	135	Wykaz infrastruktury krytycznej prowadzony przez dyrektora RCB	Wyznaczenie osoby koordynującej działania na linii operator – organy administracji publicznej, tzw. koordynatorów ochrony infrastruktury krytycznej. Wdrażanie rozwiązań w zakresie ochrony infrastruktury krytycznej.
Podmioty krytyczne świadczące usługi w sektorze energii	80	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów stosowanych obecnie w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej „ustawa k.s.c.") w odniesieniu do operatorów usług kluczowych.	Przeprowadzenie oceny ryzyka świadczonej usługi kluczowej. Wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi. Zapewnienie obsługi incydentów mających wpływ na świadczenie usługi kluczowej, w tym informowania o incydentach właściwych organów do spraw podmiotów krytycznych; Informowanie właściwych organów zarządzania kryzysowego o incydentach mających istotny wpływ na świadczenie usługi kluczowej, w przypadku gdy może to doprowadzić do sytuacji kryzysowej; Zapewnienie przeprowadzenia cyklicznych audytów wdrożonych rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi; Zapewnienie udziału struktur organizacyjnych lub pracowników w szkoleniach i ćwiczeniach, w tym ćwiczeniach z zakresu obrony cywilnej, ochrony ludności, zarządzania kryzysowego oraz obronnych; Wyznaczenie tzw. osób odpowiedzialnych za utrzymanie kontaktów z właściwymi organami do spraw

			podmiotów krytycznych oraz zapewnienie im organizacyjnych warunków realizacji funkcji.
Podmioty krytyczne świadczące usługi w sektorze transportu	40	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	j.w.
Podmioty krytyczne świadczące usługi w sektorze bankowości	10	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	Zgodnie z dyrektywą CER podmioty w tym sektorze nie muszą podlegać niektórym obowiązkom dla podmiotów krytycznych. Podmioty krytyczne z sektora bankowości i infrastruktury rynków finansowych nie stosują niektórych przepisów CER w zakresie w jakim mają obowiązek stosować rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, str. 1)
Podmioty krytyczne świadczące usługi w sektorze infrastruktury rynków finansowych	10	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	j.w.
Podmioty krytyczne świadczące usługi w sektorze zdrowia	15	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	Przeprowadzenie oceny ryzyka świadczonej usługi kluczowej. Wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi. Zapewnienie obsługi incydentów mających wpływ na świadczenie usługi kluczowej, w tym informowania o incydentach właściwych organów do spraw podmiotów krytycznych;

			Informowanie właściwych organów zarządzania kryzysowego o incydentach mających istotny wpływ na świadczenie usługi kluczowej, w przypadku gdy może to doprowadzić do sytuacji kryzysowej; Zapewnienie przeprowadzenia cyklicznych audytów wdrożonych rozwiązań, o których mowa w pkt 2; Zapewnienie udziału struktur organizacyjnych lub pracowników w szkoleniach i ćwiczeniach, w tym ćwiczeniach z zakresu obrony cywilnej, ochrony ludności, zarządzania kryzysowego oraz obronnych; Wyznaczenie tzw. osób odpowiedzialnych za utrzymanie kontaktów z właściwymi organami do spraw podmiotów krytycznych oraz zapewnienie im organizacyjnych warunków realizacji funkcji.
Podmioty krytyczne świadczące usługi w sektorze wody pitnej	70	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	j.w.
Podmioty krytyczne świadczące usługi w sektorze ścieków	10	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	j.w.
Podmioty krytyczne świadczące usługi w sektorze infrastruktury cyfrowej	40		Zgodnie z dyrektywą CER podmioty w tym sektorze nie muszą podlegać wszystkim obowiązkom przewidzianym dla podmiotów krytycznych (rozdz. III oraz IV dyrektywy CER).
Podmioty krytyczne świadczące usługi w sektorze administracji publicznej	60	Szacunki RCB oparte o wykaz jednostek sektora finansów publicznych zawarty w art. 9 pkt 1, 8, 9 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.	Przeprowadzenie oceny ryzyka świadczonej usługi kluczowej. Wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi.

			Zapewnienie obsługi incydentów mających wpływ na świadczenie usługi kluczowej, w tym informowania o incydentach właściwych organów do spraw podmiotów krytycznych. Informowanie właściwych organów zarządzania kryzysowego o incydentach mających istotny wpływ na świadczenie usługi kluczowej, w przypadku gdy może to doprowadzić do sytuacji kryzysowej. Zapewnienie przeprowadzenia cyklicznych audytów wdrożonych rozwiązań, organizacyjno-technicznych dotyczących zapewniania bezpieczeństwa świadczonej usługi. Zapewnienie udziału struktur organizacyjnych lub pracowników w szkoleniach i ćwiczeniach, w tym ćwiczeniach z zakresu obrony cywilnej, ochrony ludności, zarządzania kryzysowego oraz obronnych; Wyznaczenie tzw. osób odpowiedzialnych za utrzymanie kontaktów z właściwymi organami do spraw podmiotów krytycznych oraz zapewnienie im organizacyjnych warunków realizacji funkcji.
Podmioty krytyczne świadczące usługi w sektorze przestrzeni kosmicznej	5	Szacunek RCB oparty o decyzję Rady (WPZiB) 2021/698 z dnia 30 kwietnia 2021 r. w sprawie bezpieczeństwa systemów i usług wdrażanych, udostępnianych i użytkowanych w ramach Unijnego programu kosmicznego, które mogą mieć wpływ na bezpieczeństwo Unii, oraz uchylenia decyzji 2014/496/WPZiB.	j.w.
Podmioty krytyczne świadczące usługi w sektorze produkcji, przetwarzania i dystrybucji żywności	30	Szacunki RCB uwzględniające kryteria jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	j.w.
Podmioty krytyczne świadczące usługi w sektorze zarządzania usługami ICT	43	Szacunki RCB uwzględniające liczbę podmiotów kluczowych i podmiotów ważnych z sektora zarządzania ICT, wskazaną w projekcie ustawy nowelizującej ustawę k.s.c.	Sektor wprowadzony dla zapewnienia spójności z dyrektywą NIS2.

Podmioty krytyczne świadczące usługi w sektorze produkcji wytwarzania i dystrybucji chemikaliów i innych produktów przemysłowych	25	Szacunki RCB uwzględniające dotychczasową ilość operatorów infrastruktury krytycznej w systemie oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	Sektor wprowadzony dla zachowania spójności z dotychczasowym wykazem obiektów infrastruktury krytycznej w tym obszarze. Konieczność wprowadzenia takiego sektora wynika z analiz prowadzonych przez RCB w zakresie wykrywania zależności operatorów infrastruktury krytycznej od innych podmiotów (rozwiązania niezbędne dla wynikającej z dyrektywy CER ochrony łańcuchów dostaw).
Podmioty krytyczne świadczące usługi w sektorze usług pocztowych i kurierskich	10	Szacunki RCB uwzględniające dotychczasową liczbę operatorów infrastruktury krytycznej w systemie oraz zmiany liczbowe jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie k.s.c. w odniesieniu do operatorów usług kluczowych.	Sektor wprowadzony dla zachowania spójności z dotychczasowym wykazem obiektów infrastruktury krytycznej w tym obszarze.
Podmioty krytyczne świadczące usługi w sektorze gospodarowania odpadami	10	Szacunki RCB uwzględniające zmiany jakie mogą nastąpić przy zastosowaniu kryteriów jakie są stosowane w ustawie o KSC w odniesieniu do operatorów usług kluczowych.	Sektor wprowadzony dla zachowania spójności z dotychczasowym wykazem obiektów infrastruktury krytycznej w tym obszarze.
Organy do spraw podmiotów krytycznych	14	Maksymalna liczba organów do spraw podmiotów krytycznych, wynikająca z poszczególnych działów administracji rządowej. Liczba może być mniejsza w przypadku gdy kilka działów kierowanych będzie przez jednego ministra.	Identyfikowanie podmiotów krytycznych i ujmowanie w wykazie podmiotów krytycznych dla danego sektora lub podsektora. Współpraca z podmiotami krytycznym w zakresie obsługi incydentów istotnych. Zadania w zakresie nadzoru i kontroli podmiotów krytycznych w danym sektorze lub podsektorze. Nakładanie kar na podmioty krytyczne w danym sektorze lub podsektorze.
Ministrowie kierujący działami administracji rządowej	12		Identyfikowanie – zgodnie z kryteriami – obiektów, urządzeń lub instalacji jako infrastruktury krytycznej i przedkładanie wniosków o wpis do wykazu infrastruktury krytycznej prowadzonego przez RCB
Wojewodowie	16		j.w.
Rządowe Centrum Bezpieczeństwa	1		W obszarze infrastruktury krytycznej - opracowanie kryteriów identyfikacji infrastruktury krytycznej niezbędnej dla funkcjonowania państwa i zaspokojenia potrzeb

			obywateli oraz infrastruktury krytycznej niezbędnej dla zaspokojenie potrzeb lokalnych społeczności danego województwa. Prowadzenie wykazu infrastruktury krytycznej niezbędnej dla funkcjonowania państwa i zaspokojenia potrzeb obywateli, zgodnie z wnioskami zgłaszanymi przez ministrów wyznaczonych jako odpowiedzialnych za identyfikację infrastruktury krytycznej w poszczególnych sektorach lub podsektorach. Opracowanie minimalnych standardów w obszarach bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz zapewnienia planów ciągłości działania i odtwarzania. W obszarze podmiotów krytycznych – realizacja powierzonych obowiązków organu do spraw podmiotów krytycznych w sektorze administracji publiczna. W sytuacjach niecierpiących zwłoki - identyfikowanie – zgodnie z kryteriami – obiektów, urządzeń lub instalacji jako infrastruktury krytycznej i ujmowanie w wykazie infrastruktury krytycznej.
Wojewodowie	16		Identyfikowanie – zgodnie z kryteriami – obiektów, urządzeń lub instalacji jako infrastruktury krytycznej i ujmowanie ich w wykazach infrastruktury krytycznej na obszarze danego województwa. Współpraca z operatorami infrastruktury krytycznej ujętymi w danym wykazie infrastruktury krytycznej.
Komisja Nadzoru Finansowego	1		Identyfikowanie – zgodnie z kryteriami – obiektów, urządzeń lub instalacji jako infrastruktury krytycznej i ujmowanie ich w wykazach infrastruktury krytycznej na obszarze danego województwa. Współpraca z operatorami infrastruktury krytycznej

			ujętymi w danym wykazie infrastruktury krytycznej. W obszarze podmiotów krytycznych - realizacja powierzonych obowiązków organu do spraw podmiotów krytycznych dla sektora bankowości i infrastruktury rynków finansowych.
Sądy administracyjne			Rozpatrywanie skarg na decyzje o nałożeniu kary pieniężnej na podmiot krytyczny.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Stosownie do postanowień § 36 ust. 1 i 38 § 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny, udostępniony zostanie projekt *ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw* a właściwe podmioty bezpośrednie poinformowane o zamieszczeniu projektu.

W ramach konsultacji publicznych projekt zostanie skierowany do następujących podmiotów:

1) Business Centre Club;

2) Federacji Konsumentów;

3) Fundacji Bezpieczna Cyberprzestrzeń;

4) Fundacji ePaństwo;

5) Fundacji im. Stefana Batorego;

6) Fundacji Instytut Mikromakro;

7) Fundacji My Pacjenci;

8) Fundacji Nowoczesna Polska;

9) Fundacji Panoptykon;

10) Fundacji Projekt Polska;

11) Fundacji Pułaskiego;

12) Internet Society Poland Chapter;

13) Internet Society Poland;

14) Izby Gospodarki Elektronicznej;

15) Konfederacji Lewiatan;

16) Krajowego Związku Banków Spółdzielczych;

17) Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji;

18) Krajowej Izby Gospodarczej;

19) Krajowej Izby Gospodarki Cyfrowej;

20) Krajowej Izby Gospodarki Morskiej;

21) Krajowej Izby Komunikacji Ethernetowej;

22) Krajowej Izby Rozliczeniowej;

23) Krajowej Spółdzielczej Kasy Oszczędnościowo-Kredytowej;

24) Naczelnej Organizacji Technicznej;

25) Naczelnej Rady Zrzeszeń Handlu i Usług;

26) Polskiego Centrum Badań i Certyfikacji S.A.;

27) Polskiego Towarzystwa Informatycznego;

28) Polskiej Izby Brokerów Ubezpieczeniowych i Reasekuracyjnych;
29) Polskiej Izby Handlu;
30) Polskiej Izby Informatyki i Telekomunikacji;
31) Polskiej Izby Komunikacji Elektronicznej;
32) Polskiej Izby Producentów Urządzeń i Usług na rzecz Kolei;
33) Polskiej Izby Radiodyfuzji Cyfrowej;
34) Polskiej Izby Ubezpieczeń;
35) Polskiej Organizacji Handlu i Dystrybucji;
36) Polskiej Organizacji Niebankowych Instytucji Płatności;
37) Polskiej Rady Biznesu;
38) Polskiej Wytwórni Papierów Wartościowych;
39) Sektorowej Rady ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo;
40) Stowarzyszenia Inżynierów Telekomunikacji;
41) Stowarzyszenia Polskich Brokerów Ubezpieczeniowych i Reasekuracyjnych;
42) Towarzystwa Gospodarczego Polskie Elektrownie;
43) Związku Banków Polskich;
44) Operatorzy infrastruktury krytycznej – wszyscy.

W ramach opiniowania projekt zostanie skierowany do następujących podmiotów:
1) Prokuratorii Generalnej Rzeczypospolitej Polskiej;
2) Prezesa Urzędu Ochrony Konkurencji i Konsumentów;
3) Prezesa Urzędu Komunikacji Elektronicznej;
4) Prezesa Urzędu Ochrony Danych Osobowych;
5) Komisji Nadzoru Finansowego;
6) Rzecznika Małych i Średnich Przedsiębiorców;
7) Urzędu Zamówień Publicznych;
8) Polskiego Komitetu Normalizacyjnego;
9) Agencji Bezpieczeństwa Wewnętrznego;
10) Agencji Wywiadu;
11) Biura Bezpieczeństwa Narodowego;
12) Centralnego Biura Antykorupcyjnego;
13) Służby Kontrwywiadu Wojskowego;
14) Służby Wywiadu Wojskowego;
15) Służby Ochrony Państwa.
Wyniki zostaną omówione w raporcie z konsultacji.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	6,2	7,2	7,7	8,2	8,8	9,4	10,1	10,8	11,5	12,3	13,2	105,4
budżet państwa	6,2	7,2	7,7	8,2	8,8	9,4	10,1	10,8	11,5	12,3	13,2	105,4
JST												
pozostałe jednostki (oddzielnie)												

Wydatki ogółem	47,5	19,8	21,1	22,3	23,7	27,2	26,9	28,5	30,1	32,0	36,0	315,1
budżet państwa	47,5	19,8	21,1	22,3	23,7	27,2	26,9	28,5	30,1	32,0	36,0	315,1
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem	-41,3	-12,6	-13,4	-14,1	-14,9	-17,8	-16,8	-17,7	-18,6	-19,7	-22,8	- 209,7
budżet państwa	-41,3	-12,6	-13,4	-14,1	-14,9	-17,8	-16,8	-17,7	-18,6	-19,7	-22,8	- 209,7
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Budżet państwa w częściach poszczególnych ministrów będących organami do spraw podmiotów krytycznych, budżety wojewodów oraz RCB.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projektowane zmiany mają zapewnić środki finansowe na działania związane z realizacją ustawowych zadań nałożonych na podmioty właściwe do ich realizacji. Jako rok 0 przyjmuje się rok 2025 W przypadku zadań z zakresu planowania cywilnego - rozwiązania zawarte w ustawie wprowadzają w głównej mierze dodatkowe formalno – prawne narzędzia realizacji ustawowych obowiązków organów zarządzania kryzysowego, w ramach posiadanych na te zadania środków finansowych. Natomiast w przypadku realizacji zadań nakładanych dyrektywą CER konieczne jest de facto zdefiniowanie ich od podstaw oraz zapewnienie finansowania na odpowiednim poziomie. Dyrektywa CER wprowadza jako novum zadania dla organów do spraw podmiotów krytycznych, które to zadania wymagają zatrudnienia dodatkowego personelu i poniesienia kosztów związanych z odpowiednimi wynagrodzeniami. Ponadto konieczne jest poniesienie wydatków związanych z zapewnieniem narzędzi niezbędnych do pracy (koszty utworzenia stanowisk pracy). Zadania w zakresie obowiązków związanych z wdrożeniem rozwiązań zawartych w dyrektywie CER z punktu widzenia organu do spraw podmiotów krytycznych będą obejmować m.in. 1) identyfikację podmiotu krytycznego oraz jego ujęcie we właściwym wykazie prowadzonym przez organ do spraw podmiotów krytycznych; 2) współpracę z podmiotami krytycznym w zakresie obsługi incydentów istotnych, w tym wydawanie rekomendacji przez ministra w tym zakresie; 3) czynności nadzorcze, w tym zadania związane z kontrolą podmiotów krytycznych; 4) czynności związane z nakładaniem kar. Mając na względzie, iż tematyka zawarta w dyrektywie CER związana jest nierozerwalnie z tematyka ochrony infrastruktury krytycznej – należy przyjąć możliwość maksymalnie efektywnego wykorzystania obecnego potencjału kadrowego urzędów obsługujących przyszłe organy do spraw podmiotów krytycznych. Dlatego można przy zwiększonych obowiązkach podmiotów przyjęto założenie minimalne w postaci dodania 3 etatów w odniesieniu do każdego z sektorów, z wyłączeniem sektora administracja publiczna. Przy 14 wyodrębnionych sektorach daje to liczbę **42 nowych etatów**. Przez analogię należy potraktować koszty związane z realizacją nowego zadania dla wojewodów dotyczącego identyfikacji obiektów, urządzeń oraz instalacji jako infrastruktury krytycznej. Dlatego też wskazane jest dokonanie zwiększenia zatrudnienia w wszystkich urzędach wojewodów o 1 etat, co daje łącznie **16 nowych etatów**. Jednostkowe wyliczenie etatu – jako podstawę wyliczeń przyjęto stanowisko głównego specjalisty, mnożnik kwoty bazowej 3,5 oraz 20% dodatek stażowy. Uwzględniono wynagrodzenie roczne oraz koszty pracodawcy, tj. składkę na ubezpieczenie społeczne oraz składkę na Fundusz Pracy i Fundusz Solidarnościowy. Łącznie – roczny koszt pracownika wyniesie **169 810, 83 zł**. Uwzględniając fakt, że wzrost przeciętnego wynagrodzenia w gospodarce krajowej wyniósł w ostatnich 10 latach około 7,01% - proponuje się przyjąć taką prognozę wynagrodzeń dla

	następnych 10 lat. Dlatego też przy łącznej liczbie **58 etatów** zbiorowe koszty roczne w perspektywie 10 lat kształtują się następująco: 1) rok 2025 – 9 195 909,76 zł (wyliczenie nie zawiera kosztów rocznego wynagrodzenia) 2) rok 2026 – 10 622 195,36 zł 3) rok 2027 – 11 366 811,26 zł 4) rok 2028 – 12 163 624,73 zł 5) rok 2029 – 13 016 294,82 zł 6) rok 2030 – 13 928 737,09 zł 7) rok 2031 – 14 905 141,56 zł 8) rok 2032 – 15 949 991,98 zł 9) rok 2033 – 17 068 086,42 zł 10) rok 2034 – 18 264 559,28 zł 11) rok 2035 – 19 544 904,88 zł Mając na względzie łączną liczbę **58 etatów** przy koszcie jednostkowym 12 000 zł daje to kwotę 696 000 zł na rok 2025, na zakup ww. sprzętu. Przy uwzględnieniu zużycia sprzętu i konieczności jego wymiany proponuje się analogiczną kwotę ująć w budżecie co 5 lat. W przypadku Rządowego Centrum Bezpieczeństwa – należy przyjąć fakt, że po raz pierwszy instytucja będzie zapewniała pełną obsługę organu do spraw podmiotów krytycznych w sektorze administracji publicznej (Prezesa Rady Ministrów), z wyłączeniem nakładania kar administracyjnych. Wiąże się to z koniecznością rozbudowania struktur organizacyjnych, w głównej mierze w na potrzeby wykonywania czynności związanych ze sprawowaniem nadzoru nad realizacją przepisów ustawy w sektorze administracja publiczna. Poza tym należy mieć na względzie, że RCB będzie również koordynować współpracę międzynarodową w zakresie realizacji postanowień dyrektywy CER, w tym prowadzić Pojedynczy Punkt Kontaktowy, czy też zapewniać reprezentację kraju na forum Grupy do spraw Odporności Podmiotów Krytycznych. Nie bez znaczenia pozostaje również obsługa prawna procesów realizowanych w ramach realizacji dyrektywy CER. Planowane jest więc powstanie wydziału dedykowanego zadaniom w zakresie nadzoru nad realizacją przepisów ustawy, wzmocnienie kadrowe obsługi współpracy międzynarodowej oraz rozbudowa obsługi prawnej RCB, m.in. w przypadku konieczności prowadzenia postępowań przed sądami administracyjnymi. Nowe zadania w zakresie oceny ryzyka i kwestii zarządzania ryzykiem wymagają uzupełnienia potencjału kadrowego RCB. W tym obszarze, obok „standardowych" prac planistycznych konieczne będzie znaczące rozbudowanie zadań o procesy gromadzenia i analizy informacji, które są niezbędne do skutecznego zarządzania ryzykiem. Powyższe zadania nie mogą odbywać się bez zapewnienia całodobowego, efektywnego, obiegu informacji oraz obsługi strony teleinformatycznej wszystkich procesów. Obecna sytuacja finansowa jak i stan kadrowy uniemożliwia efektywne wykonywanie obowiązków w tym zakresie. Proponowane zmiany w zakresie zatrudnienia i kosztów z tym związanych dostosowano adekwatnie do przyszłych potrzeb. Planowane zwiększenie stanu osobowego RCB o **35 etatów**, co powinno zapewnić właściwą realizację przyszłych zadań. Jednostkowe wyliczenie etatu - jako podstawę wyliczeń stanowisko głównego specjalisty, przy maksymalnej stawce w tej kategorii zaszeregowania oraz 20% dodatek stażowy. Uwzględniono wynagrodzenie roczne oraz koszty pracodawcy, tj. składkę na ubezpieczenie społeczne oraz składkę na Fundusz Pracy i Fundusz Solidarnościowy. Łącznie – roczny koszt pracownika wyniesie **160 583, 90 zł.** Uwzględniając fakt, że wzrost przeciętnego wynagrodzenia w gospodarce krajowej wyniósł w ostatnich 10 latach około 7,01% - proponuje się przyjąć taką prognozę wynagrodzeń dla

następnych 10 lat.

1) rok 2025 – 5 247 728,64 zł
2) rok 2026 – 6 061 651,35 zł
3) rok 2027 – 6 486 573,11 zł
4) rok 2028 – 6 941 281,89 zł
5) rok 2029 – 7 427 865,75 zł
6) rok 2030 – 7 948 559,14 zł
7) rok 2031 – 8 505 753,13 zł
8) rok 2032 – 9 102 006,43 zł
9) rok 2033 – 9 740 057,08 zł
10) rok 2034 – 10 422 835,08 zł
11) rok 2035 – 11 153 475,82 zł

Dodatkowo należy wskazać koszty związane z wyjazdami osób odpowiedzialnych za współpracę międzynarodową szacowane na 444 400,00 zł rocznie (założenie 4 osoby, 44 wyjazdy na rok, po dwa dni). Obejmują one wyjazdy zagraniczne w ramach współpracy z właściwymi podmiotami UE w zakresie realizacji zadań UMOL oraz w ramach współpracy w zakresie realizacji postanowień CER (oraz zbliżonych tematycznie kwestii odporności w NATO).
Maksymalne koszty wyjazdy zespołu kontrolnego złożonego z 3 kontrolerów, przy 6 kontrolach rocznie, trwających do 5 dni, wyniosą rocznie 47 250,00 zł.

Mając na względzie łączną liczbę 35 etatów przy koszcie jednostkowym 12 000 zł daje to kwotę 420 000 zł na rok 2025, na zakup ww. sprzętu. Przy uwzględnieniu zużycia sprzętu i konieczności jego wymiany proponuje się analogiczną kwotę ująć w budżecie co 5 lat.

Ponadto koszty zabezpieczenia teleinformatycznego realizacji zadań obejmują:

1) wymianę sprzętu w serwerowni - 770 000,00 zł co 5 lat;
2) utrzymanie zapasowej serwerowni oraz wydzielonego systemu kopii zapasowych – 110 000,00 na rok;
3) aktualizację oprogramowania serwerowego – 180 000,00 zł co 3 lata
4) aktualizację i utrzymanie urządzeń typu Firewall oraz innych urządzeń bezpieczeństwa sieci IT; 150 000 na rok
5) aktualizacje oprogramowania odpowiedzialnego za cyberbezpieczeństwo (Antywirus, EDR/XDR, PAM, 2FA, SCCM, VEEAM itp.) – 400 000,00 na rok;
6) utrzymanie usług Internetowych wraz systemem Anty DDoS - 35 000,00 zł na rok;
7) aktualizacje oprogramowania użytkowego – biurowego – 125 000,00 zł na rok
8) zakupy wynikające z nieoczekiwanych sytuacji oraz naprawy i wsparcie w trakcie awarii – 200 000,00 zł na rok;
9) modyfikacja wyposażenia niezbędnego do prowadzenia posiedzeń Rządowego Zespołu Zarządzania Kryzysowego oraz Zespołu ds. Incydentów Krytycznych – ok 3 000 000 zł (koszt jednorazowy);
10) utworzenie i zapewnienie funkcjonowania systemu teleinformatycznego wykorzystywanego jako narzędzie wspierające realizację zadań zarządzania kryzysowego – koszt utworzenia 25 000 000 zł oraz roczne koszty utrzymania i eksploatacji w kolejnych latach 1 000 000 zł rocznie począwszy od roku 2025. Kwota utrzymania i eksploatacji w kolejnych latach wzrasta o wskaźnik CPI (wytyczne dotyczące stosowania jednolitych wskaźników makroekonomicznych będących podstawą oszacowania skutków finansowych projektowanych ustaw. Aktualizacja - maj 2024 r.).

Jako dochody budżetu państwa należy wskazać składki na ubezpieczenie społeczne finansowane przez pracodawcę oraz składki na Fundusz Pracy i Fundusz Solidarnościowy.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł,	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							

ceny stałe z …… r.)	rodzina, obywatele oraz gospodarstwa domowe							

W ujęciu niepieniężnym	duże przedsiębiorstwa	W celu wdrożenia projektowanych przepisów przedsiębiorstwa muszą wdrożyć środki techniczne i organizacyjne proporcjonalne do wielkości podmiotu oraz rodzaju prowadzonej działalności. Przedsiębiorcy powinni oszacować swoje posiadane zasoby tak aby zbudować system bezpieczeństwa świadczonej usługi z ich wykorzystaniem, bez generowania nadmiernych kosztów. Przy budowie bezpieczeństwa usługi kluczowej niezbędne jest systematyczne szacowanie ryzyka wystąpienia incydentu oraz odpowiednie zarządzanie ryzykiem. Takie działanie pozwoli na wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych. Istotne będzie również zbudowanie obiegu informacji o incydentach lub możliwościach ich wystąpienia, zarządzania incydentami oraz stosowania środków zapobiegawczych jak również ograniczających wpływ incydentów na świadczenie usługi kluczowej.
	sektor mikro-, małych i średnich przedsiębiorstw	Brak możliwości oszacowania wpływu nowych regulacji na przedsiębiorców. Projekt oddziałuje na podmioty o zróżnicowanej wielkości – od małych do dużych przedsiębiorstw. Jakiej wielkości przedsiębiorstwa zostaną objęte reżimem ustawy – będzie to uzależnione od uzgodnienia parametrów progów istotności skutku zakłócającego.
	rodzina, obywatele oraz gospodarstwa domowe	Projektowane regulacje przyczynią się do zwiększenia bezpieczeństwa świadczenia usług, z których korzystają obywatele. Na obecnym etapie brak jest możliwości oszacowania kosztów.
Niemierzalne		

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Oszacowanie kosztów przedsiębiorców w zakresie dostosowania się do nowych regulacji nie jest możliwe. Środki techniczne i organizacyjne wdrażane przez przedsiębiorców będą uzależnione od oceny ryzyka, która będzie przeprowadzana dopiero po ujęciu przedsiębiorcy w wykazie podmiotów krytycznych w danym sektorze. Obecnie wielu przedsiębiorców, będących właścicielami lub posiadaczami infrastruktury krytycznej wdraża systemy zarządzania bezpieczeństwem lub ciągłością działania zgodnie z obowiązującymi w tym zakresie normami lub posiada certyfikację zgodności z tymi normami. Nakładane obowiązki na przedsiębiorców są konieczne i niezbędne dla osiągnięcia celów ustawy – należy uznać, iż została tu zachowana zasada proporcjonalności.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	x zwiększenie liczby dokumentów x zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz:
Ustawa powoduje zmianę kształtu obecnie opracowywanych dokumentów planistycznych. Krajowa Ocena Ryzyka zastąpi Raport o zagrożeniach bezpieczeństwa narodowego.
Przewiduje się cykliczne sporządzanie streszczenia istotnych elementów krajowej oceny ryzyka oraz streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem.
Sporządzone zostaną w nowej formule plany zarządzania kryzysowego na wszystkich szczeblach administracji publicznej.

W odniesieniu do infrastruktury krytycznej – opracowane zostaną kryteria wyłaniania infrastruktury krytycznej.
Operator infrastruktury krytycznej będzie sporządzał raport o stanie ochrony infrastruktury krytycznej. W celu realizacji

zadań w zakresie ochrony infrastruktury krytycznej - operatorzy powołają koordynatorów. Do uprawnień koordynatora, któremu operator zapewnia warunki do wykonywania zadań, zalicza się m.in. możliwość przedkładania rekomendacji organowi zarządzającemu operatora w zakresie ochrony jego obiektów, instalacji urządzeń i usług.
Ponadto przewidziano, iż operator infrastruktury krytycznej w związku z realizacją przedsięwzięć w zakresie ochrony jego obiektów, instalacji, urządzeń i usług zapewnia zdolność do ochrony informacji niejawnych. Należy bowiem przyjąć, że informacje wrażliwe wytworzone w ramach opracowywania, uzgadniania oraz realizacji dokumentacji dotyczącej ochrony infrastruktury krytycznej oraz informacje wymieniane z właściwymi organami administracji publicznej o zidentyfikowanych zagrożeniach lub zakłóceniach infrastruktury krytycznej oraz podejmowanych działaniach w celu jej ochrony lub odtworzenia, powinny być klasyfikowane jako informacje niejawne. Regulacja, zgodnie z postanowieniami ustawy o ochronie informacji niejawnych, pozostawia operatorom infrastruktury krytycznej decyzję co do sposobów zapewnienia ochrony informacji niejawnych, w zależności od poziomu niejawności wytwarzanych informacji.

W odniesieniu do podmiotów krytycznych w poszczególnych sektorach lub podsektorach – ze strony organów do spraw podmiotów krytycznych konieczne będzie:
1) wdrożenie procesów ich identyfikacji oraz ujmowania w odpowiednich wykazach;
2) prowadzenie wykazów, w tym ich bieżąca aktualizacja;
3) wdrożenie procedur audytu i kontroli podmiotów krytycznych
4) wdrożenie procedur dotyczących nakładania kar na podmioty krytyczne.

Ze strony podmiotów krytycznych konieczne będzie wdrażanie rozwiązań związanych z bezpieczeństwem świadczenia usługi kluczowej czy tez przeprowadzenie cyklicznych audytów.

9. Wpływ na rynek pracy

Projektowane rozwiązania wpłyną pozytywnie na rynek pracy. Nowe regulacje przewidują obowiązek wyznaczania przez podmioty krytyczne tzw. osób odpowiedzialnych za utrzymanie kontaktów z właściwymi organami do spraw podmiotów krytycznych oraz zapewnienie im organizacyjnych warunków realizacji funkcji. W praktyce przełoży się to na zwiększone zapotrzebowanie na usługi specjalistów z zakresu kompleksowego zapewnienia bezpieczeństwa oraz ciągłości świadczenia usług. Wpłyną one również pozytywnie na firmy świadczące usługi z zakresu audytu.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny x sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	Projekt ustawy przewiduje nakładanie kar pieniężnych. Skargi na decyzje administracyjne w sprawie nałożenia kary będą rozpatrywały sądy administracyjne.

11. Planowane wykonanie przepisów aktu prawnego

Wykonanie przepisów ustawy nastąpi po dniu jej wejścia w życie.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

W odniesieniu do rozwiązań w obszarze planowania cywilnego - ewaluacja będzie odbywać się w formie ćwiczeń z zakresu zarządzania kryzysowego, testujących rozwiązania zawarte w dokumentach planistycznych oraz kontrole realizacji zadań/przedsięwzięć przeprowadzane przez uprawnione do tego podmioty (np. kontrole prowadzone przez NIK).

W przypadku rozwiązań dotyczących podmiotów krytycznych świadczących usługi kluczowe, możliwe do zastosowania mierniki to m.in. liczba podmiotów wpisanych do wykazu podmiotów krytycznych, liczba zgłoszonych incydentów istotnych w danym roku kalendarzowym, liczba przeprowadzonych audytów przez podmioty krytyczne oraz liczba nałożonych administracyjnych kar pieniężnych.
Powyższe mierniki powinny dać odpowiedź na pytanie, czy i w jaki sposób przepisy ustawy są stosowane.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
Brak załączników.