Nr ewidencji bibliot. 849/NJ/2/Zał. 1/60

EGZEMPLARZ NADZOROWANY

Metodyka szacowania ryzyka

Zintegrowany System Zarządzania

Sporządził:		Zatwierdził:	
Pełnomocnik ds. ZSZ	mgr inż. Mirosław Dereń	Dyrektor	płk dr n. med. Alicja TROCHIMIUK
Podpis:		Podpis:	
Data :	17.03.2022 r.	Data :	21 MAR. 2022
Wydanie:	6.1	Wydanie 1.0 wprowadzone zostało Zarządzeniem Dyrektora WIML Nr 12/2011	

Cel i zakres

Celem opracowania metodyki zarządzania ryzykiem w ramach Zintegrowanego Systemu Zarządzania (ZSZ) jest ustanowienie sposobu:

- identyfikacji,
- oceny
- oraz postępowania z ryzykiem

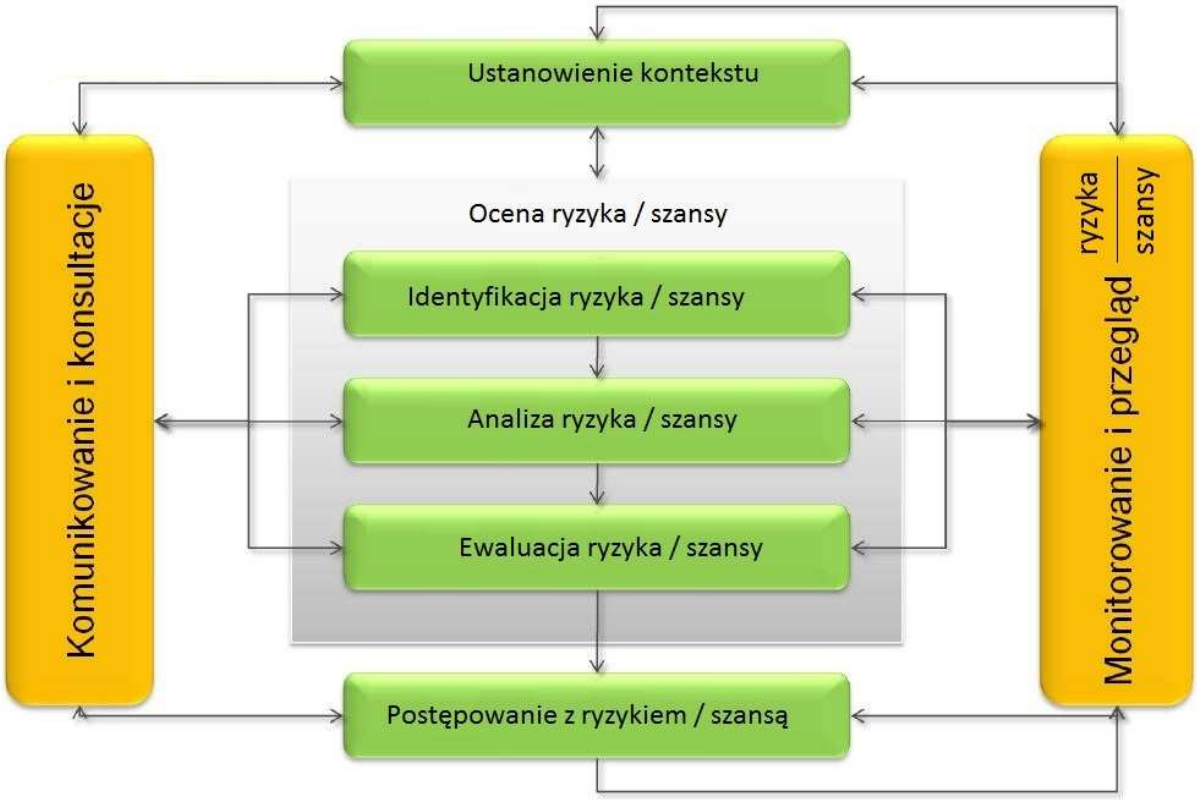
w procesach biznesowych Wojskowego Instytutu Medycyny Lotniczej (WIML) związanych z realizacją zadań statutowych, takich jak planowanie działalności, zawieranie umów i ich realizacją, zgodnie z wymaganiami norm ISO 27001:2017, ISO 9001:2015, AQAP 2110:2016 oraz z wymaganiami Ministra Obrony Narodowej w sprawie planowania i rozliczania działalności w resorcie obrony narodowej (Dz.Urz.MON.2014.179 z późn. zm.).

Podstawowe pojęcia

Bezpieczeństwo informacji	-	zachowanie poufności, integralności i dostępności informacji, co oznacza że informacja nie jest ujawniana osobom nieupoważnionym, jest ona dokładna i kompletna oraz jest dostępna w użytecznej formie na żądanie upoważnionego personelu
Zarządzanie ryzykiem i szansą	-	skoordynowane działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka lub szansy
Ryzyko	-	wpływ niepewności na możliwość zrealizowania celu – niedowartościowane ryzyko może pociągnąć za sobą szkodę w organizacji (pośrednio lub bezpośrednio)
Ryzyko bezpieczeństwa informacji	-	potencjalnie możliwa sytuacja, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów powodując w ten sposób powstanie szkody w komórkach organizacyjnych (w organizacji).
Szansa	-	wpływ niepewności podczas określania celu - niedowartościowana szansa może ograniczyć możliwą do uzyskania korzyść. Przewartościowana szansa może skutkować brakiem możliwości uzyskania przewidywanej korzyści ze zrealizowanego celu.
Niepewność	-	określa wielkość obszaru (w metrologii - przedziału wartości mierzonej) dla której można uznać, że prawdopodobieństwo osiągnięcia założonego celu jest na zadowalającym poziomie. Niepewność to stan, również częściowy, braku informacji związanej ze zrozumieniem lub wiedzą na temat ewentualnego zdarzenia, jego następstw lub prawdopodobieństwa jego wystąpienia.
Aktywa	-	wszystko to, co ma wartość dla komórek organizacyjnych (dla Instytutu) – w metodyce obejmuje też: procesy / zadania
Rejestr ryzyka	-	dokument, o którym mowa w Regulaminie systemu kontroli zarządczej
Zdarzenie	-	efekt (skutek) zmaterializowania się zagrożenia

Proces zarządzania ryzykiem i szansą

Działalność Wojskowego Instytutu Medycyny Lotniczej obejmuje wiele obszarów, które muszą być uwzględnione podczas analizy kontekstu organizacji.
Wynik analizy kontekstu należy uwzględnić w procesie planowania działalności bieżącej WIML.` Planowanie to powinno uwzględnić ryzyka ujęte w rejestrze ryzyka, o którym mowa w wymaganiach Ministra Obrony Narodowej w sprawie planowania i rozliczania działalności w resorcie obrony narodowej (Dz.Urz.MON.2014.179 z późn. zm.). W wyniku analizy kontekstu, oprócz ryzyk, mogą być wskazane szanse. Należy rozważyć czynniki wpływające na ryzyka i szanse, a następnie postępować z nimi zgodnie ze schematem przedstawionym na Rys. 1, umożliwiającym wypracowanie podstawy do podjęcia działań w poszczególnych obszarach mających zapewnić osiągnięcie przyjętego celu.
Dalsza część dokumentu zawiera:
metodę analizy ryzyka spełniającą wymagania Regulaminu kontroli zarządczej;
metodę analizy ryzyka (ryzyk cząstkowych) przyjętą w WIML dla obszarów objętych systemem;
metodę analizy ryzyka przyjętą do stosowania w Planach Jakości Wyrobu.

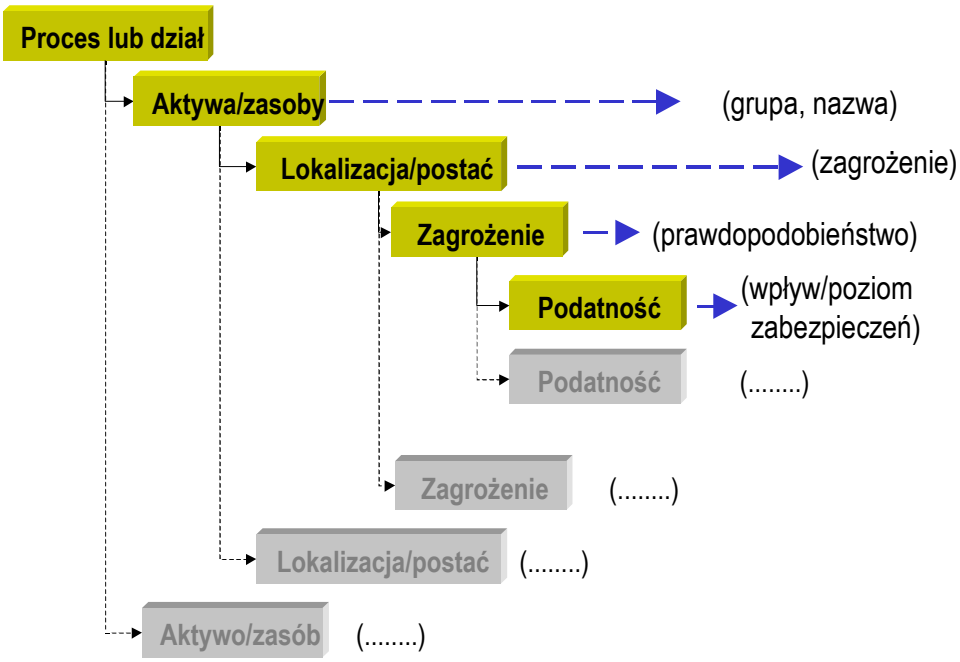


Rys. 1 Schemat postępowania ryzykiem lub szansą.

Elementy ryzyka

W metodyce uwzględniono:

– aktywa / procesy / zadania / cele,
– wartość (istotność) aktywów / procesów / zadań / celów,
– lokalizację/postać aktywów,
– potencjalne zagrożenia,
– prawdopodobieństwa wystąpienia tych zagrożeń,
– podatności aktywów / procesów / zadań / celów na zagrożenia,
– wpływ zagrożeń na bezpieczeństwo aktywów / procesów / zadań / celów,
– skuteczność zastosowanych zabezpieczeń
– zadania / procesy.



Rys. 2. Schematyczna struktura elementów ryzyka

Przebieg procesu zarządzania ryzykiem

Zarządzanie ryzykiem należy rozpocząć od jego identyfikacji. Następnie należy wyróżnić istotne cechy danego ryzyka, takie jak obszar, którego dotyczy, prawdopodobieństwo wystąpienia, wpływ skutków wystąpienia zdarzenia.

Ze względu na odmienne wymagane cele analizy ryzyka i oczekiwaną przejrzystość wyników analizy niezbędne jest wyróżnienie trzech metod analizy ryzyka w WIML związanego z:

1) zapewnieniem ciągłości informacji (dostępność, integralność, poufność),
2) realizacją odrębnej umowy, zawartej z wymaganiami AQAP 2110:2016.
3) planowaniem działalności Instytutu na okres realizacji zadania lub na nadchodzący najbliższy rok planistyczny,

Cele analizy są określone są przez obszary i dotyczą:

1) procesów realizowanych w organizacji oraz ocena ich wpływu na funkcjonowanie organizacji. Wskazana wartość wpływu określa, na ile zaburzenia funkcjonowania procesu mogą spowodować zaburzenia funkcjonowania organizacji,
2) realizacji poszczególnych umów zawartych w oparciu o wymagania normy AQAP 2110:2016,
3) planowania i realizacji planów działalności bieżącej Instytutu.

1. Zasady postępowania z ryzykiem dla zapewnienia ciągłości informacji

Do zaklasyfikowania wielkości wpływu zagrożenia na funkcjonowanie Instytutu (skutek, wpływ na biznes) należy zastosować kryteria zawarte w Tabeli 1.

Tabela 1. Wpływ zdarzenia na funkcjonowanie Instytutu (skutek, wpływ na biznes)

Ocena	Współczynnik **W**	**Opis**
Krytyczny	5	utrata lub naruszenie bezpieczeństwa komórki organizacyjnej lub procesu powoduje przerwanie ciągłości działalności Instytutu, utrata lub naruszenie bezpieczeństwa danych osobowych lub procesu powoduje wysokie straty majątkowe i niemajątkowe dla osoby, której dane dotyczą, kradzież tożsamości i utratę kontroli nad swoimi danymi osobowymi,
Poważny	4	utrata lub naruszenie bezpieczeństwa komórki organizacyjnej lub procesu powoduje przerwanie ciągłości działalności komórki organizacyjnej Instytutu, utrata lub naruszenie bezpieczeństwa danych osobowych lub procesu może mieć negatywny wpływ na prawa i wolności osób, których dane dotyczą, np. poprzez utratę kontroli nad danymi osobowymi, stratę majątkową bądź niemajątkową,
Duży	3	utrata lub naruszenie bezpieczeństwa komórki organizacyjnej lub procesu może mieć negatywny wpływ na ciągłość działalności Instytutu utrata lub naruszenie bezpieczeństwa danych osobowych lub procesu może mieć negatywny wpływ na prawa i wolności osób, których dane dotyczą, np. poprzez utratę kontroli nad danymi osobowymi, stratę niemajątkową
Znaczący	2	utrata lub naruszenie bezpieczeństwa komórki organizacyjnej lub procesu powoduje utrudnienia w normalnym funkcjonowaniu Instytutu utrata lub naruszenie bezpieczeństwa danych osobowych lub procesu ma duży wpływ na prawa i wolności osób, których dane dotyczą, np. poprzez stratę niemajątkową
Mały	1	utrata lub naruszenie bezpieczeństwa komórki organizacyjnej lub procesu ma ograniczony wpływ na funkcjonowanie Instytutu utrata lub naruszenie bezpieczeństwa danych osobowych lub procesu ma ograniczony wpływ na prawa i wolności osób, których dane dotyczą

gdzie pozycja „Krytyczny” oznacza wpływ największy, a „Mały” – wpływ najmniejszy.

Aktywa - identyfikacja

Kluczowym elementem zarządzania ryzykiem są aktywa / procesy cele. Oznacza to, że należy przeprowadzić identyfikację aktywów / procesów / celów w komórkach organizacyjnych objętych systemem i określić ich wartość dla Instytutu.
Lista przykładowych aktywów znajduje się w Załączniku 1.

Identyfikacja zagrożeń

Aby zabezpieczyć aktywa lub zasoby, należy wiedzieć, przed czym, czyli jakie zagrożenia mogą wystąpić w przypadku konkretnego działania lub aktywa. Dobrą praktyką jest wskazywanie przede wszystkim rzeczywistych zagrożeń – tzn. takich, które mogą wystąpić i występują w organizacji (konkretne awarie, braki zasilania, nieuprawnione przekazanie informacji, kradzież), a nie tylko takich, które łatwo wymienić (zamach terrorystyczny, zrzut paliwa przez lądujące awaryjnie samoloty - tam gdzie nie ma lotniska) itp. Z punktu widzenia kompletności szacowania ryzyka powinna być brana pod uwagę jak największa liczba zagrożeń (również tych mało prawdopodobnych). Jednak należy pamiętać, że istotnym elementem procesu analizy ryzyka jest możliwość uzyskania aktualnych i miarodajnych wyników. Zbyt rozbudowana analiza – o mniej istotne elementy – może spowodować, że w momencie jej zakończenia będzie już nieaktualna.
Lista przykładowych zagrożeń i podatności znajduje się w Załączniku 2.

Określenie prawdopodobieństwa

Nie wszystkie zagrożenia występują tak samo często lub są tak samo prawdopodobne, stąd wprowadzone zostało pojęcie prawdopodobieństwa wystąpienia zagrożenia. Awarie urządzeń, czy brak zasilania są na pewno częstsze niż pożary czy powodzie i podtopienia pomieszczeń. Do oceny prawdopodobieństwa należy zastosować skalę pięciostopniową: Olbrzymie, Wielkie, Duże, Niewielkie, Małe. Dla każdego poziomu prawdopodobieństwa przypisano wartość współczynnika oceny prawdopodobieństwa. Skala ta opisana jest w Tabeli 2.

Określenie podatności dla aktywów informacyjnych

Kolejnym elementem zarządzania ryzykiem są podatności, czyli słabe strony naszych aktywów - cechy i / lub właściwości aktywa, które mogą zostać wykorzystane przez zagrożenie, co zwiększyć może prawdopodobieństwo wystąpienia zdarzenia w szczególnych okolicznościach. Papier chronimy przez spaleniem, ponieważ nie jest odporny na ogień – wprost przeciwnie - jest podatny na spalenie. Komputer niezabezpieczony hasłem powoduje, że zawarte w nim dane osobowe lub wrażliwe dane medyczne są podatne na utratę poufności (zdobycie wiedzy przez nieuprawnione osoby), integralności (usunięcie lub zmianę niektórych zapisów), dostępności (usunięcie lub zaszyfrowanie wszystkich zapisów).

Tabela 2. Ocena prawdopodobieństwa wystąpienia zagrożenia

Ocena	Współczynnik P_p	Opis	
Olbrzymie	20	występuje często (np. raz w miesiącu) lub regularnie z ustaloną częstotliwością, lub jest bardzo prawdopodobne;	>90%
Wielkie	15	występuje względnie często (np. raz na kwartał) lub regularnie z ustaloną częstotliwością, lub jest prawdopodobne;	76-90%
Duże	10	wystąpiło w ostatnim roku, zdarza się nieregularnie, lub istnieje realne prawdopodobieństwo wystąpienia;	41-75%
Niewielkie	5	nie wystąpiło ani razu w ciągu ostatniego roku lub jest mało prawdopodobne;	10-40%
Małe	1	nie wystąpiło ani razu w ciągu ostatniego roku lub jest mało prawdopodobne;	<10%

gdzie wartość współczynnika „Olbrzymie” związany jest z prawdopodobieństwem najwyższym, a „Małe” – najniższym.

Określenie podatności dla aktywów informacyjnych

Kolejnym elementem zarządzania ryzykiem są podatności, czyli słabe strony naszych aktywów - cechy i / lub właściwości aktywa, które mogą zostać wykorzystane przez zagrożenie, co zwiększyć może prawdopodobieństwo wystąpienia zdarzenia w szczególnych okolicznościach. Papier chronimy przez spaleniem, ponieważ nie jest odporny na ogień – wprost przeciwnie - jest podatny na spalenie. Konkretne urządzenie jest zagrożone wystąpieniem awarii, ponieważ pracuje 24 h na dobę (podatność – ciągła praca) lub w trudnych warunkach (podatność – trudne warunki pracy: zapylenie, inne).
Lista przykładowych zagrożeń i podatności znajduje się w Załączniku 2.
Wyróżniono trzy grupy podatności charakterystyczne dla aktywów informacyjnych. Są to:

1) poufność - S_p,
2) integralność - S_i,
3) dostępność – S_d.

W niniejszej metodyce przyjęto jednakową skalę oceny podatności dla każdej z trzech ww. cech (Tabela 3). Podatności mogą wpływać łącznie na poziom ryzyka (patrz wzór nr 3), co należy uwzględnić w analizie ryzyka związanego z aktywami informacyjnymi.

Tabela 3. Ocena podatności wpływających na poufność, integralności, dostępności

Ocena.	Współczynnik S_p, S_i, S_d	Opis
Istotna	1	aktywa o określonych cechach znajdują się lub będą się znajdować przez nieokreślony okres czasu w otoczeniu sprzyjającym wystąpieniu zdarzenia;
Pomijalna	0	cechy aktywa i jego otoczenie nie sprzyjają wystąpieniu zdarzenia

Należy dokonać oceny wpływu zagrożenia na poufność, integralność i dostępność (bezpieczeństwo informacji) oraz należy określić poziom skuteczności wdrożonych zabezpieczeń. Są to elementy domykające prowadzoną analizę. Skala oceny poziomów zabezpieczeń określona jest w Tabeli 4.

Tabela 4. Poziom zabezpieczeń

Ocena	Współczynnik **Z**	**Opis**
Wysoki	4	występujące zabezpieczenie chroni skutecznie przed znanymi zagrożeniami,
Znaczący	3	występują częściowe zabezpieczenia, które chronią tylko wybrane obszary, ale są w pełni skuteczne
Średni	2	występują częściowe zabezpieczenia, które chronią tylko wybrane obszary, ale nie są w pełni skuteczne
Pomijalny	1	praktycznie brak jest jakichkolwiek zabezpieczeń lub są one mało skuteczne

gdzie: poziom „Wysoki” oznacza najwyższą wartość (najwyższy poziom zabezpieczeń) i może osiągnąć wartość „∞”. Jednak na tym etapie skuteczności zabezpieczeń przyjęto wartość „4”. Poziom „Pomijalny” oznacza najniższą wartość (najniższy poziom zabezpieczeń).

Określenie ryzyka i ryzyka szczątkowego

Ryzyko aktywa (też: procesu / zadania / celu) stanowi podstawę do oceny realnej utraty bezpieczeństwa tego aktywa na tle pozostałych aktywów w sytuacji, kiedy nie stosujemy jeszcze żadnych zabezpieczeń. Lista aktywów, uporządkowana wg ich ryzyk, stanowi podstawę do określenia, jakie zabezpieczenia powinny być wybrane w celu ochrony najbardziej ryzykownych aktywów.

W celu uzyskania porównywalnych ze sobą ryzyk aktywów, przyjmuje się ogólnie następujący sposób ich obliczania. Ażeby obliczyć ich wartość należy podstawić do poniższego wzoru wartości liczbowe przypisane do poszczególnych pozycji. Wielkości nie są istotne, ważna jest ich powtarzalność.

Podstawą do wyliczeń ryzyka aktywa jest następujący wzór (1):

$$R = P * W \quad (1)$$

gdzie:

R – ryzyko aktywa / procesu / zadania / celu

P – prawdopodobieństwo wystąpienia zagrożenia (wartość wskaźnika)

W – wpływ (skutek) zmaterializowania się zagrożenia

$$P = P_p * (1 + S) \quad (2)$$

gdzie: S – podatność aktywa / procesu / zadania / celu

P_p – prawdopodobieństwo wystąpienia zagrożenia

$$S = S_p + S_i + S_d \quad (3)$$

gdzie: S_p, S_i, S_d – podatności aktywa informacyjnego, odpowiednio na: poufność, integralność, dostępność.

Po wyborze i wdrożeniu zabezpieczeń należy ponownie przeprowadzić szacowanie ryzyka, ale już z uwzględnieniem poziomów zabezpieczeń, jakie zostały zapewnione dzięki wdrożonym zabezpieczeniom. Dla każdego aktywa, po uwzględnieniu zabezpieczeń, należy obliczyć ryzyko szczątkowe.

Ryzyko szczątkowe, zgodnie z ogólnie przyjętą zasadą obliczane jest wg następującego wzoru (4):

$$R_s = R / Z \quad (4)$$

gdzie:

R_s – ryzyko szczątkowe aktywa / procesu / zadania

R – ryzyko aktywa / procesu / zadania

Z – skuteczność zastosowanych zabezpieczeń

Na podstawie uzyskanych ryzyk szczątkowych aktywów kierownictwo określa i akceptuje poziom „ryzyka akceptowalnego”, jako ustaloną wartość ryzyka, poniżej którego ryzyka aktywów zostają uznane za akceptowalne.

Kryteria akceptacji ryzyka i poziom ryzyka akceptowalnego aktywów informacyjnych

Niezbędnym elementem procesu szacowania ryzyka jest określenie „kryteriów oceny ryzyka”, czyli przyjętego podejścia do podziału ryzyk na ryzyka możliwe do zaakceptowania oraz na ryzyka nieakceptowalne.

W niniejszej metodyce **przyjęto, jako kryterium akceptacji ryzyka, dążenie do wyrównania poziomów ryzyk dla wszystkich aktywów, zgodnie z zasadą, że o sile systemu bezpieczeństwa świadczy jego najsłabszy (najbardziej ryzykowny) element**. Aktywa o ryzykach poniżej wartości wyznaczonej przez odcięcie „kominów ryzyka” obarczone są ryzykiem na takim poziomie, że kierownictwo Instytutu gotowe jest je obecnie zaakceptować (ryzyko szczątkowe akceptowalne - R_{sA}).

Poziom ryzyka akceptowalnego (R_{sA}) jest konkretną wartością ryzyka, na wykresie zaznaczony linią poziomą przechodzącą przez punkt na osi ryzyka, który zostaje wyznaczony zgodnie z kryteriami akceptacji ryzyka. Poziom ryzyka akceptowalnego powinien być określany dla każdej przeprowadzonej analizy ryzyka z uwzględnieniem trzech poziomów znaczenia skutków. Należy określić największą, graniczną wartość dla ryzyka szczątkowego akceptowalnego (R_{sA}). Przykład z określoną wartością graniczną ryzyka przedstawia Tabela 5. Macierz kwantyfikacji ryzyka zwaną także macierzą ryzyk grupującą wartości ryzyk przedstawia Rys. 3.

Tabela 5. Wartości graniczne wskaźnika grupujące ryzyko (R) **i ryzyko szczątkowe** (R_s)

Wskaźnik poziomu ryzyka				
R		**R_s** - ocena bieżąca	**R_s** –kolejne planowane okresy	
1	**niski**			
3				
4				
5	**średni**			**Akceptowalny - R_{sA}**
8				**Nieakceptowalny - R_{sN}**
9				
10	**wysoki**		**Akceptowalny - R_{sA}**	
12			**Nieakceptowalny - R_{sN}**	
15		**Akceptowalny - R_{sA}**		
16	**krytyczny**	**Nieakceptowalny - R_{sN}**		
50				
100				

R_S	R_W	R_W	**R_K**	**R_K**
R_N	R_S	R_W	**R_K**	**R_K**
R_N	R_S	R_S	R_W	R_W
R_N	R_N	R_S	R_S	R_W
R_N	R_N	R_N	R_N	R_S

Rys. 3 Macierz ryzyk (R), gdzie: R_N - ryzyko niskie, R_S **-** ryzyko średnie, R_W - ryzyko wysokie, R_K - ryzyko krytyczne,

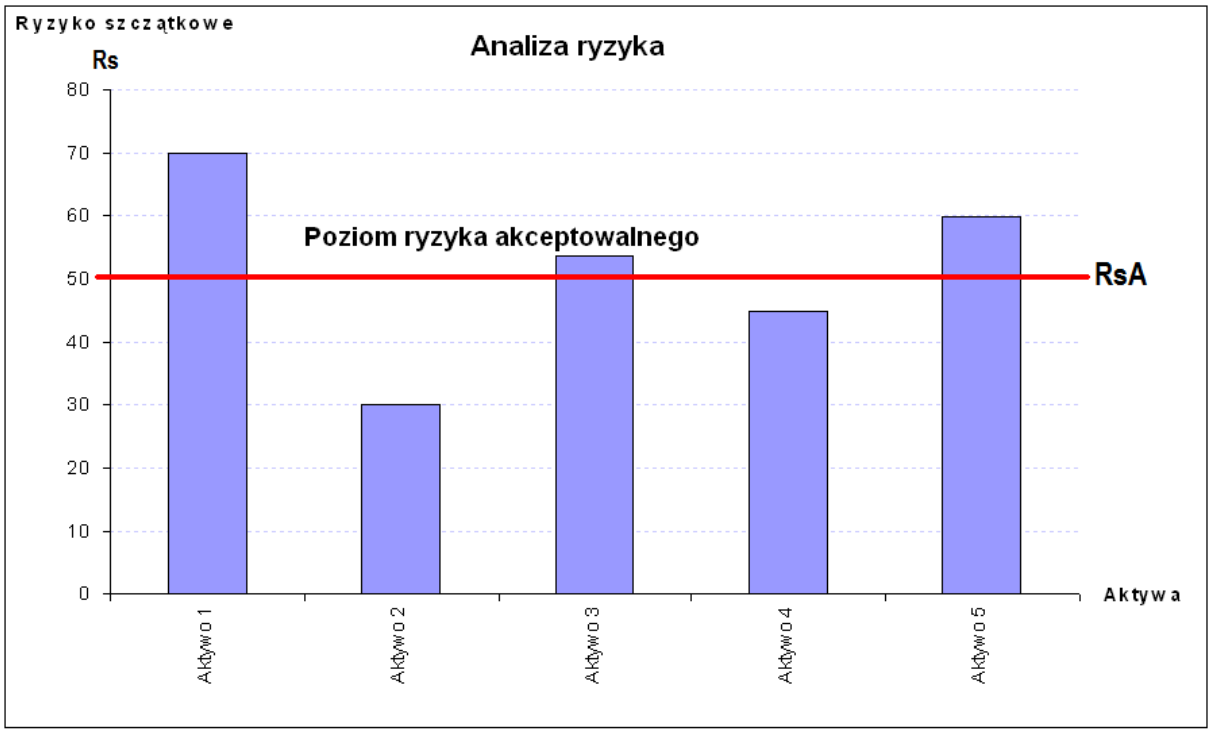
Wytyczne szczegółowe do analizy, szacowania i postępowania z ryzykiem dla aktywów informacyjnych

Analiza ryzyka powinna obejmować wszystkie obszary funkcjonowania Instytutu mające wpływ na realizowane procesy i być przygotowywana przy współudziale osób reprezentujących:

- procesy główne,
- Dyrekcję Instytutu,
- Pion Głównego Księgowego,
- Pion Administracyjny (z wyłączeniem Pracowni Informatyki),
- Pracownię Informatyki,
- Pion Ochrony.

Analizę ryzyka należy przeprowadzać okresowo, w przypadku planowanych zmian organizacyjnych, a także w terminach wyznaczonych przez Pełnomocnika ds. ZSZ.
Właściciele procesów głównych są odpowiedzialni za przygotowanie cząstkowych analiz ryzyka, obejmujących aktywa w swoim obszarze i przekazanie ich do Pełnomocnika ds. Zintegrowanego Systemu Zarządzania, który po scaleniu uzyska łączny wynik analizy dla obszaru Instytutu objętego systemem.
Do analizy ryzyka należy wykorzystać arkusz kalkulacyjny udostępniany na stronie intranetowej WIML, w zakładce formularzy ZSZ w formie pliku elektronicznego (Sygn. WIML-ZSZ-46).

Jako wynik procesu szacowania należy wykonać wykaz aktywów najbardziej zagrożonych w Instytucie. Umożliwia on podjęcie decyzji, dla których aktywów należy w pierwszej kolejności wdrożyć zabezpieczenia (fizyczne, techniczne lub organizacyjne). Wyniki analizy mogą być dla Dyrekcji podstawą do określenia poziomu ryzyka akceptowalnego (RsA) oraz do oceny zasadności przydzielenia środków na zabezpieczenie najważniejszych aktywów, co umożliwia przygotowanie planu, mającego na celu obniżenie ryzyk szczątkowych aktywów, których ryzyko szczątkowe jest większe od ustalonej wartości ryzyka akceptowalnego.
Graficzną prezentację poziomu ryzyka akceptowalnego należy wykonać w postaci wykresu dla aktywów najbardziej zagrożonych (Rys. 4).
Określenie poziomu ryzyka akceptowalnego kończy etap szacowania ryzyka.



Rys. 4 Wynik szacowania ryzyka z określonym poziomem akceptowalnego ryzyka szczątkowego (R_sA).

Plan postępowania z ryzykiem należy przygotować zgodnie ze wzorem formularza (Sygn. WIML-ZSZ-5) i dołączyć do Raportu z analizy ryzyka.

2. Zasady zarządzania ryzykiem zgodnie z wymaganiami AQAP 2110.

Przeprowadzenie analizy czynników mających wpływ na realizację umów realizowanych przez Instytut zgodnie z wymaganiami AQAP 2110

Celem analizy jest identyfikacja ryzyk związanych z realizacją umów zawartych z MON, realizowanych w obszarach objętych systemem. Oszacowanie ryzyk związanych z realizacją umów umożliwia stronom umowy zarządzanie ryzykiem.

Jakościowa analiza czynników ryzyka

W celu określenia poziomu ryzyk realizacji umowy ze względu na dany czynnik ryzyka stosujemy macierz kwantyfikacji ryzyka zwaną także macierzą ryzyk (Rys. 5), gdzie:

Poziom ryzyka = Prawdopodobieństwo * Wpływ na realizację umowy

Do oceny prawdopodobieństwa należy zastosować skalę opisaną w Tabeli 2.

Do oceny wpływu na realizację umowy (skutków urzeczywistnienia się ryzyka) należy przyjąć kryteria zawarte w Tabeli 6.

Tabela 6. Wpływ na realizację umowy

Ocena	Wartość	Opis
Krytyczny	4	utrata lub naruszenie bezpieczeństwa komórki organizacyjnej lub procesu powoduje przerwanie realizacji umowy
Wielki	3	utrata lub naruszenie bezpieczeństwa komórki organizacyjnej lub procesu może mieć negatywny wpływ na termin realizacji umowy
Znaczący	2	utrata lub naruszenie bezpieczeństwa komórki organizacyjnej lub procesu powoduje utrudnienia w normalnym trybie realizacji umowy
Normalny	1	utrata lub naruszenie bezpieczeństwa komórki organizacyjnej lub procesu ma ograniczony wpływ na realizację umowy

gdzie pozycja „Krytyczny” oznacza wpływ największy, a „Normalny” – wpływ najmniejszy.

MACIERZ RYZYK

prawdopodopodobieństwo / wpływ	Normalny	Znaczący	Wielki	Krytyczny
Olbrzymie	S 5	W 10	W 15	W 20
Wielkie	S 4	S 8	W 12	W 16
Duże	N 3	S 6	S 9	W 12
Niewielkie	N 2	S 4	S 6	S 8
Małe	N 1	N 2	N 3	S 4

Linia tolerancji ryzyka

Rys. 5 Macierz ryzyk dla przyjętych w niniejszej metodyce: wartości wskaźników prawdopodobieństw (Tabela 2) i wartości wskaźników wpływu zagrożenia (Tabela 6). Poziom ryzyka: Niski (ozn. „N”); Średni (ozn. „S”); Wysoki (ozn. „W”).

Przyjęto następującą, ogólną zasadę doboru strategii dla oszacowanych ryzyk realizacji umowy:

- **wysoki poziom ryzyka (10÷20)** – należy stosować najbardziej kosztowne i złożone plany. Dla negatywnych unikanie tj. doprowadzenie do sytuacji, że dany czynnik ryzyka nie ma możliwości wystąpić. Należy również przeanalizować wycofanie*);

- dla ryzyk o **średnim poziomie ryzyka (4÷9)** mniej kosztowne, ale także mniej skuteczne plany wprowadzenia zabezpieczeń łagodzących czyli zmniejszających prawdopodobieństwo i/lub skutki ryzyka;
  Dla **wysokich i średnich poziomów** ryzyka można również stosować strategię: przeniesienia. Najczęściej przeniesienie ryzyka polega na ubezpieczeniu się od jakiegoś zdarzenia lub scedowanie skutków ryzyka na kontrahenta (lub podwykonawcę);
- dla ryzyk o **niskim poziomie (1÷3)** stosuje się zazwyczaj akceptację ryzyk. Jeżeli zagrożenia się ziszczą ponosimy odpowiednie skutki. Akceptację dzielimy na aktywną (posiadamy rezerwę finansową) i pasywną (brak rezerw).

Przykład oszacowania ryzyk

W Tabeli 7 pokazano przykładowe aktywa / procesy, określono zagrożenia, wartości wskaźników prawdopodobieństwa wystąpienia zdarzeń. Wyliczono wartości ryzyka dla każdego aktywa / procesu.

Tabela 7. Ryzyka związane z realizacją umowy

Aktywa/Procesy	Symbol	Zagrożenie	Prawdo-podobieństwo	Wpływ zagrożenia	Ryzyko
Internet (sieć LAN)	LAN	zerwanie linii	1	1	1
Symulatory	Sym	kradzież	5	1	5
Badanie barofunkcji	Bar	nieżyt górnych dróg oddechowych	3	2	6
Personel techniczny	Te	absencja	3	2	6
…	?	…	…	…	…
Symulatory	Sym	awaria	3	5	15

Na macierz ryzyka naniesiono symbole aktywów / procesów, umieszczając je w polach macierzy zgodnie z wyliczonymi wartościami (Rys. 6).

*) Wycofanie – strategia wykorzystywana w początkowej fazie projektu. Np. przeprowadzenie studium wykonalności. Sprawdzamy czy rezultat projektu (dostarczany produkt lub usługa) ma szanse na spełnienie założonych wymagań. Jeśli nie - ponieśliśmy koszty na badania, ale inwestycja nie pochłonie bezsensownie całego budżetu.

MACIERZ RYZYK

Olbrzymie	**S** **Kom** (5)	W 10	**W** **Sym** (15)	W 20
Wielkie	S 4	S 8	W 12	W 16
Duże	N 3	**S** **Te, Bar** (6)	S 9	W 12
Niewielkie	N 2	S 4	S 6	S 8
Małe	**N** **LAN (1)**	N 2	N 3	S 4
prawdopodobieństwo / wpływ	**Normalny**	**Znaczący**	**Wielki**	**Krytyczny**

Linia tolerancji ryzyka

Rys. 6 Macierz ryzyk - przykład.

Powyższa, przykładowa macierz ryzyk uwidacznia ryzyko o symbolu „Sym” ponad linią tolerancji ryzyka, w obszarze wysokiego ryzyka. Należałoby zatem, zgodnie z przyjętymi zasadami dokonać np. przygotowanie drugiego, zastępczego symulatora. Dla aktywów „Te”, „Kom” i procesu „Bar” należałoby zastosować środki zapobiegawcze (ograniczające prawdopodobieństwo wystąpienia lub wpływ zagrożenia). Dla aktywa o symbolu „LAN” można by zaakceptować związane z nim ryzyko.

3. Zasady postępowania z ryzykiem podczas planowania działalności Instytutu.

Podczas planowania działalności bieżącej Instytutu prowadzonej zgodnie z Zarządzeniem Dyrektora WIML Nr 15/2019 z dnia 28.11.2019 r. należy przeprowadzić analizę ryzyka związanego z realizacją planowanych celów. (Kopię Zarządzenia dołączono do niniejszej metodyki).

Celem analizy jest identyfikacja ryzyk związanych z realizacją zadań wynikających z planu działalności bieżącej.

Zidentyfikowane ryzyka należy opisać w Rejestrze ryzyka, o którym mowa w punkcie 15 Art. 3 Decyzji Nr 218/MON („rejestr ryzyka - dokument, o którym mowa w Regulaminie systemu kontroli zarządczej"). Regulamin systemu kontroli zarządczej jest Załącznikiem do Decyzji Nr 93 Dyrektora Generalnego Ministerstwa Obrony Narodowej z dnia 23 lipca 2014 r. (Przykładowy wzór rejestru ryzyka do planu działalności Instytutu dołączono do niniejszej metodyki).

Określenie ryzyka

Ryzyko celu (też: procesu / zadania) stanowi podstawę do oceny możliwości realizacji celu w sytuacji, kiedy nie stosujemy jeszcze żadnych zabezpieczeń. Ryzyko celu stanowi podstawę do określenia, jakie zabezpieczenia powinny być wybrane aby cel mógł być zrealizowany.
Aby określić poziom ryzyka dla przyjętego celu należy wykorzystać wzory 1, 2 i 3 opisane w punkcie pierwszym metodyki.

Postępowanie z ryzykiem należy opisać w Rejestrze ryzyka wypełniając zawarte w nim pola.

Załącznik 1

Aktywa - przykłady

- Informacje
  - Niezbędne do funkcjonowania Instytutu
  - Wrażliwe - dane osobowe, dane medyczne
  - Strategiczne decydujące dla rozwoju Instytutu
  - Istotne, o wysokim koszcie pozyskania, przechowywania lub przetwarzania
- Sprzęt i wyposażenie
  - Sprzęt mobilny (laptopy, PDA itp.)
  - Sprzęt stały (serwery, komputery osobiste)
  - Peryferia (drukarki, przenośne napędy itp.)
  - Masowe pamięci (macierze, urządzenia kopii zapasowych)
  - Nośniki danych (CD, taśma, pendrive, dysk zewnętrzny)
- Oprogramowanie
  - Systemy operacyjne
  - Oprogramowanie serwisowe i administracyjne
  - Oprogramowanie standardowe lub grupowe (bazy danych, serwery, praca grupowa)
  - Aplikacje biznesowe
    - Standardowe
    - Specyficzne
- Sieci
  - Elementy pośredniczące (router, hub, switch)
  - Interfejsy komunikacyjne (GPRS, karty sieciowe)
- Pracownicy
  - Kierownictwo i właściciele aktywów
  - Użytkownicy sprzętu przetwarzającego informacje
  - Administratorzy (systemów , baz danych, systemów bezpieczeństwa)
  - Lekarze
  - Instruktorzy
  - Pielęgniarki, personel techniczny
- Lokalizacja
  - Otoczenie zewnętrzne
  - Teren,
  - Kluczowe usługi
  - Komunikacja, obieg informacji
  - Wyposażenie (klimatyzacja, dostawa wody, wywóz śmieci itp.)
- Organizacja
  - Organy administracji
  - Struktura organizacyjna
  - Klienci

Załącznik 2

Lista zagrożeń i podatności

Przykłady obszarów narażonych na zagrożenia

Poniższa lista podaje przykłady obszarów narażonych na zagrożenia, znajdujących się w różnych rejonach bezpieczeństwa, włączając w to przykłady zagrożeń, które mogą takie obszary wykorzystać. Lista ta może być pomocna przy szacowaniu obszarów narażonych.
Zaznacza się, iż mogą istnieć inne zagrożenia będące w stanie wykorzystać te obszary narażone na zagrożenia.

Bezpieczeństwo personelu

- Absencja personelu - niedobór kadry
- Nie nadzorowana praca wykonywana przez kadry zewnętrzne lub sprzątające – kradzież
- Niewystarczające szkolenie w zakresie bezpieczeństwa – błędy kadry wsparcia operacyjnego
- Brak świadomości w zakresie bezpieczeństwa – błędy użytkowników
- Słabo udokumentowane oprogramowanie – błędy kadry wsparcia operacyjnego
- Brak mechanizmów monitorowania – używanie oprogramowania w sposób nieupoważniony
- Brak polityk prawidłowego użytkowania mediów telekomunikacyjnych i systemów powiadamiania tego typu – używanie infrastruktury sieciowej w sposób nieautoryzowany
- Niewłaściwe procedury rekrutacyjne – rozmyślne szkody

Bezpieczeństwo fizyczne i środowiskowe

- Niewłaściwe lub niedbałe prowadzenie kontroli dostępu fizycznego do budynków, pomieszczeń i biur – rozmyślne szkody
- Brak fizycznej ochrony budynków, drzwi i okien – kradzież
- Lokalizacja w rejonie podatnym na zalania – powódź
- Niechronione magazynowanie – kradzież
- Niewystarczająca konserwacja / wadliwa instalacja nośników – utrata informacji
- Brak planów okresowej wymiany sprzętu – spadek jakości nośników
- Podatność sprzętu na wilgotność, pył, zabrudzenie – lotne cząstki / pył – niestabilna praca
- Podatność sprzętu na wahania temperatury – ekstremalne temperatury
- Podatność sprzętu na wahania napięcia – wahania zasilania – utrata informacji
- Niestabilna sieć zasilająca – wahania zasilania –wyłączenia sprzętu

Zarządzanie komputerami i sieciami

- Niechronione linie komunikacyjne – podsłuch
- Wadliwie połączone okablowanie – infiltracja łączności
- Brak mechanizmów identyfikacji i upoważniania – podszywanie się pod tożsamość użytkownika
- Transfer haseł w otwartej sieci – dostęp dla nieupoważnionych użytkowników
- Brak dowodu wysłania lub otrzymania wiadomości – odrzucenie reklamacji
- Sieć oparta na łączach komutowanych - dostęp dla nieupoważnionych użytkowników
- Niechroniony przesył poufnych danych – podsłuch, kopiowanie danych
- Pojedynczy punkt awarii – awaria usług komunikacyjnych
- Niewłaściwe zarządzanie siecią – przeciążenie ruchu
- Brak troski podczas rozporządzania materiałami – kradzież
- Niekontrolowane kopiowanie – kradzież danych
- Niezabezpieczone połączenia z sieci publicznych – używanie oprogramowania przez nieupoważnionych użytkowników – wyciek danych

Kontrola dostępu do systemu / opracowywanie i utrzymywanie systemu

- Skomplikowany interfejs użytkownika – błąd personelu operacyjnego
- Pozbywanie się lub ponowne użytkowanie nośników bez odpowiednich procedur usuwania danych – korzystanie z oprogramowania przez osoby nieupoważnione
- Brak dziennika kontroli – korzystanie z oprogramowania w sposób nieautoryzowany
- Brak dokumentacji – błąd działania personelu
- Brak efektywnych zabezpieczeń zmian – wady oprogramowania
- Brak mechanizmów identyfikacji i autoryzacji, takich jak autoryzacja użytkownika – podszywanie pod tożsamość użytkownika
- Niewylogowanie się przy odejściu od stacji roboczej – korzystanie z oprogramowania przez osoby nieupoważnione
- Brak lub niewystarczające testowanie oprogramowania - korzystanie z oprogramowania przez osoby nieupoważnione
- Niewydolne zarządzanie hasłami (łatwe do odgadnięcia hasła, przechowywanie haseł, zbyt rzadka wymiana haseł) – podszywanie się pod tożsamość użytkownika
- Niejasne lub niepełne specyfikacje dla twórców oprogramowania – wady oprogramowania
- Niekontrolowane pobieranie plików i korzystanie z oprogramowania – złośliwe oprogramowanie
- Niechronione tabele haseł – podszywanie się pod tożsamość użytkownika
- Dobrze znane usterki w oprogramowaniu – korzystanie z oprogramowania przez osoby nieupoważnione
- Błędne przyznawanie uprawnień dostępowych – korzystanie z oprogramowania w sposób nieautoryzowany

Podatności

1. Środowisko i infrastruktura

– Brak fizycznej ochrony budynku, drzwi i okien
(może zostać wykorzystana na przykład przez zagrożenie kradzieżą)
– Niewłaściwe lub nieuważne użycie fizycznej kontroli dostępu do budynków, pomieszczeń
(może zostać wykorzystana na przykład przez zagrożenie umyślną szkodą)
– Niestabilna sieć elektryczna
(może zostać wykorzystana na przykład przez zagrożenie wahaniami natężenia prądu)
– Lokalizacja na terenie zagrożonym powodzią
(może zostać wykorzystana na przykład przez zagrożenie zalaniem)

2. Sprzęt

– Brak planów okresowej wymiany
(może zostać wykorzystana na przykład przez zagrożenie zużyciem nośników)
– Podatność na zmiany napięcia
(może zostać wykorzystana na przykład przez zagrożenie wyłączenia urządzenia)
– Podatność na zmiany temperatury
(może zostać wykorzystana na przykład przez zagrożenie wyłączenia urządzenia)
– Podatność na wilgotność, kurz, zabrudzenie
(może zostać wykorzystana na przykład przez zagrożenie przegrzania wyłączenia urządzenia)
– Wrażliwość na promieniowanie elektromagnetyczne
(może zostać wykorzystana na przykład przez zagrożenie uszkodzenie nośników danych)
– Niewłaściwa konserwacja / wadliwa instalacja nośników
(może zostać wykorzystana na przykład przez zagrożenie uszkodzenie nośników danych
– Brak sprawnej kontroli zmian w konfiguracji
(może zostać wykorzystana przez zagrożenie uszkodzenie oprogramowania lub danych)

3. Oprogramowanie

– Niejasny lub niekompletny opis techniczny dla projektantów
(może zostać wykorzystana na przykład przez zagrożenie uszkodzeniem oprogramowania)
– Brak lub niedostateczne przetestowanie oprogramowania
(może zostać wykorzystana na przykład przez zagrożenie użyciem oprogramowania przez nieuprawnionych użytkowników)
– Skomplikowany interfejs użytkownika
(może zostać wykorzystana na przykład przez zagrożenie błędem zapisu danych)
– Brak mechanizmów identyfikacji i uwierzytelniania takich jak uwierzytelnianie użytkowników
(może zostać wykorzystana na przykład przez zagrożenie kradzieżą tożsamości użytkownika)
– Brak możliwości audytu
(może zostać wykorzystana na przykład przez zagrożenie ukrytych błędów oprogramowania)
– Dobrze znane wady oprogramowania
(może zostać wykorzystana na przykład przez zagrożenie użyciem oprogramowania przez nieuprawnionych użytkowników)
– Niechronione tablice haseł

(może zostać wykorzystana na przykład przez zagrożenie kradzieżą tożsamości użytkownika)

- Złe zarządzanie hasłami
  (hasła łatwe do odgadnięcia, przechowywanie haseł w postaci jawnej, zbyt rzadkie zmiany - może zostać wykorzystana na przykład przez zagrożenie kradzieżą tożsamości użytkownika)
- Niewłaściwy przydział uprawnień do dostępu
  (może zostać wykorzystana na przykład przez zagrożenie użyciem oprogramowania w nieuprawniony sposób)
- Brak kontroli pobierania i używania oprogramowania
  (może zostać wykorzystana na przykład przez zagrożenie złośliwym oprogramowaniem)
- Brak konieczności wylogowania się po opuszczeniu stacji roboczej
  (może zostać wykorzystana na przykład przez zagrożenie użyciem oprogramowania przez nieuprawnionych użytkowników)
- Brak efektywnej kontroli zmian
  (może zostać wykorzystana na przykład przez zagrożenie awarią oprogramowania)
- Brak dokumentacji
  (może zostać wykorzystana na przykład przez zagrożenie błędem obsługi)
- Brak kopii zapasowych
  (może zostać wykorzystana na przykład przez zagrożenie brakiem możliwości odtworzenia danych)
- Usuwanie lub ponowne użycie nośników bez odpowiedniego kasowania ich zawartości
  (może zostać wykorzystana na przykład przez zagrożenie użycia oprogramowania przez nieuprawnionych użytkowników)

4. Łączność

- Niechronione linie łączności
  (może zostać wykorzystana na przykład przez zagrożenie podsłuchem)
- Złe łączenie kabli
  (może zostać wykorzystana na przykład przez zagrożenie infiltracją łączności)
- Brak identyfikacji i uwierzytelniania nadawcy i odbiorcy
  (może zostać wykorzystana na przykład przez zagrożenie podszyciem się pod użytkownika)
- Przesyłanie haseł w postaci jawnej
  (może zostać wykorzystana na przykład przez zagrożenie dostępu do sieci przez nieuprawnionych użytkowników)
- Brak dowodu wysłania lub odebrania wiadomości
  (może zostać wykorzystana na przykład przez zagrożenie zaprzeczenia)
- Linie komutowane
  (może zostać wykorzystana na przykład przez zagrożenie dostępu do sieci przez nieuprawnionych użytkowników)
- Niechroniony wrażliwy ruch
  (może zostać wykorzystana na przykład przez zagrożenie podsłuchem)
- Nieodpowiednie zarządzanie siecią (odporność trasowania na uszkodzenia)
  (może zostać wykorzystana na przykład przez zagrożenie przeciążeniem ruchem)

– Niechronione połączenia do sieci publicznej
  (może zostać wykorzystana na przykład przez zagrożenie użyciem oprogramowania przez nieuprawnionych użytkowników)

5. Dokumenty

– Niechronione przechowywanie
  (może zostać wykorzystana na przykład przez zagrożenie kradzieżą)
– Nieodpowiednie niszczenie
  (może zostać wykorzystana na przykład przez zagrożenie kradzieżą)
– Niekontrolowane kopiowanie
  (może zostać wykorzystana na przykład przez zagrożenie kradzieżą)

6. Personel

– Nieobecność personelu
  (może zostać wykorzystana na przykład przez zagrożenie niewykonaniem zadań)
– Praca personelu zewnętrznego lub sprzątającego bez nadzoru
  (może zostać wykorzystana na przykład przez zagrożenie kradzieżą)
– Niedostateczne szkolenia w zakresie bezpieczeństwa
  (może zostać wykorzystana na przykład przez zagrożenie wypadkiem przy pracy)
– Brak świadomości bezpieczeństwa
  (może zostać wykorzystana na przykład przez zagrożenie błędami użytkowników)
– Niewłaściwe użycie oprogramowania i sprzętu
  (może zostać wykorzystana na przykład przez zagrożenie uszkodzenia sprzętu)
– Brak mechanizmów monitorowania
  (może zostać wykorzystana na przykład przez zagrożenie użyciem oprogramowania w nieuprawniony sposób)
– Brak polityk właściwego użycia środków łączności i komunikowania się
  (może zostać wykorzystana na przykład przez zagrożenie użyciem instalacji sieciowych w nieuprawniony sposób)
– Niewłaściwe procedury zatrudniania
  (może zostać wykorzystana na przykład przez zagrożenie realizacji zadań)

7. Podatności mające zastosowanie ogólne

– Pojedynczy punkt uszkodzenia
  (może zostać wykorzystana na przykład przez zagrożenie awarią usług łączności)
– Niewłaściwa reakcja serwisu dokonującego konserwacji
  (może zostać wykorzystana na przykład przez zagrożenie spowodowania awarii sprzętu

Wykaz zmian

Lp.	Data zmiany	Nr strony	Krótki opis zmiany	Wprowadził
Zmiany w wydaniu 6.0				
1	16.03.2022	5	Tabela 1 Zmieniono nazwy skali zagrożeń	M. Dereń
2	16.03.2022	7	Tabela 2 Zmieniono nazwy skali i współczynniki prawdopodobieństwa	M. Dereń
3	16.03.2022	8	Tabela 4 Zmieniono współczynniki poziomu zabezpieczeń	M. Dereń
4	16.03.2022	9	Zmieniono wzór nr 2 i uzupełniono opis użytych symboli	M. Dereń
5	16.03.2022	16	Punkt 3 Dodano informacje o dodatkowych, wspomagających, nienumerowanych załącznikach do metodyki.	M. Dereń
6	16.03.2022	23	Usunięto str. nr 23 – Załącznik 3 –Plan postępowania z ryzykiem (Form. WIML-ZSZ-5-w.1)	M. Dereń
7	17.03.2022	6	Ostatnie zdanie. Zmieniono treść. Podano przykłady dotyczące podatności danych osobowych.	M. Dereń
Zmiany w wydaniu 6.1				
1				
2				
3				
4				
5				
6				
7				

WOJSKOWY INSTYTUT
MEDYCYNY LOTNICZEJ

ZARZĄDZENIE Nr 15 /2019
DYREKTORA
WOJSKOWEGO INSTYTUTU MEDYCYNY LOTNICZEJ
z dnia 28.11.2019 r.

w sprawie planowania i rozliczania działalności bieżącej
w Wojskowym Instytucie Medycyny Lotniczej

§ 1.

Na podstawie Statutu Wojskowego Instytutu Medycyny Lotniczej (Dz.Urz.MON.2017.198), Decyzji Nr 218/MON Ministra Obrony Narodowej z dnia 6 czerwca 2014 r. w sprawie planowania i rozliczania działalności w resorcie obrony narodowej (Dz.Urz.MON.2014.179 z późn. zm.), zwanej dalej „Decyzją Nr 218/MON", oraz w oparciu o normy: ISO 9001:2015 „Systemy zarządzania jakością – Wymagania" i normy ISO 27001:2017 „Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania", w celu ujednolicenia zasad planowania i rozliczania działalności bieżącej w Wojskowym Instytucie Medycyny Lotniczej, zwanym dalej „Instytutem", zarządza się co następuje:

1. Sporządzać w WIML następujące dokumenty dotyczące planowania działalności:
   1.1. Roczny plan działalności Instytutu na rok planistyczny,
   1.2. Kwartalny plan zasadniczych przedsięwzięć Instytutu,
   1.3. Plan szkolenia uzupełniającego Kadry Instytutu.
2. Roczny plan działalności Instytutu opracowywać do 25 listopada roku przedplanowego i przedstawiać Dyrektorowi Instytutu do zatwierdzenia do 30 listopada roku przedplanowego, a następnie do 10 grudnia roku przedplanowego przedstawić do zatwierdzenia Dyrektorowi Departamentu Wojskowej Służby Zdrowia Ministerstwa Obrony Narodowej.
   2.1 Roczny plan działalności Instytutu należy sporządzać na podstawie decyzji, rozkazów i wytycznych Dyrektora Departamentu Wojskowej Służby Zdrowia, analizy kontekstu Instytutu oraz propozycji kierowników organizacyjnych Instytutu.
   2.2 Wzór rocznego planu działalności Instytutu określa Załącznik 1 do niniejszego zarządzenia (formularz WIML-WAP-19-w.1).
   2.3 Kolejne wydania formularza o którym mowa w ppkt. 2.2 mogą być wprowadzane na podstawie decyzji Szefa Pionu Administracyjnego WIML.
2.4 Razem z planem działalności na rok planistyczny należy opracowywać do 25 listopada roku przedplanowego i przedstawiać do zatwierdzenia do 30 listopada roku przedplanowego Dyrektorowi Instytutu rejestr ryzyka, który następnie należy przedstawić wraz z planem działalności na rok planistyczny Dyrektorowi Departamentu Wojskowej Służby Zdrowia Ministerstwa Obrony Narodowej.

2.5 Rejestr ryzyka jest to dokument, o którym mowa w punkcie 15 art. 3 Decyzji Nr 218/MON („rejestr ryzyka - dokument, o którym mowa w Regulaminie systemu kontroli zarządczej").

3. Kwartalny plan zasadniczych przedsięwzięć Instytutu, opracowany przez Kierownika Wydziału Administracyjno-Personalnego i zatwierdzony przez Szefa Pionu Administracyjnego przedstawiać Dyrektorowi Instytutu do zatwierdzenia w terminie do 28 dnia miesiąca poprzedzającego rozpoczęcie kwartału.
   Przy opracowywaniu propozycji do kwartalnego planu zasadniczych przedsięwzięć należy stosować następujące zasady:
   3.1 Do kwartalnego planu zasadniczych przedsięwzięć Instytutu nie wprowadzać zadań przewidzianych do realizacji w sposób ciągły.
   3.2 W przypadku, gdy zadanie ujęte w planie działalności Instytutu trwa kilka miesięcy, do kwartalnego planu zasadniczych przedsięwzięć należy wpisywać termin rozpoczęcia i zakończenia zadania oraz jego wyznaczone etapy.
   3.3 Wzór kwartalnego planu zasadniczych przedsięwzięć określa załącznik nr 8 do Decyzji Nr 218/MON.
   Oryginał kwartalnego planu zasadniczych przedsięwzięć Instytutu, na którym zostały naniesione adnotacje o realizacji zamierzeń, należy przekazywać do akt w terminie do ostatniego dnia miesiąca po zakończeniu kwartału.
4. Plan szkolenia uzupełniającego Kadry Instytutu, sporządzony przez wyznaczonego żołnierza zawodowego (nieetatowego kierownika szkolenia uzupełniającego), należy przedstawić Dyrektorowi Instytutu do zatwierdzenia w terminie do 3 grudnia roku przedplanowego.
   4.1 Wzór planu szkolenia uzupełniającego kadry określa załącznik nr 9 do Decyzji Nr 218/MON.
5. W ramach rozliczania działalności w WIML polecam Szefowi Pionu Administracyjnego:
   5.1 W terminie do 3 lutego - sprawozdanie roczne z wykonania planu działalności za rok poprzedni przedstawić Dyrektorowi Instytutu do zatwierdzania.
   5.2 W terminie do 10 lutego - zatwierdzone sprawozdanie roczne z wykonania planu działalności za rok poprzedni przekazać Dyrektorowi Departamentu Wojskowej Służby Zdrowia Ministerstwa Obrony Narodowej.
   5.3 W terminie do 3 lipca - sprawozdanie półroczne z wykonania planu działalności w roku planistycznym przedstawić Dyrektorowi Instytutu do zatwierdzania.
   5.4 W terminie do 10 lipca - zatwierdzone sprawozdanie półroczne z wykonania planu działalności w roku planistycznym przekazać Dyrektorowi Departamentu Wojskowej Służby Zdrowia Ministerstwa Obrony Narodowej.
   5.5 Wzór sprawozdania z wykonania planu działalności załącznik nr 10 do Decyzji Nr 218/MON.

§ 2.

1. Zobowiązuję Kierownika Wydziału Administracyjno-Personalnego do umieszczenia treści niniejszego zarządzenia na stronie intranetowej WIML i do poinformowania o tym szefów oraz kierowników pionów i komórek organizacyjnych WIML (dopuszczalna jest forma powiadomienia elektronicznego).
2. Zobowiązuję szefów i kierowników pionów i komórek organizacyjnych WIML do zapoznania z niniejszym zarządzeniem wszystkich podwładnych pracowników i żołnierzy (dopuszczalna jest forma powiadomienia elektronicznego).

§ 3

1. Zarządzenie niniejsze wchodzi w życie z dniem podpisania.
2. Z dniem wejścia w życie niniejszego zarządzenia traci moc Zarządzenie Dyrektora WIML Nr 31/16 z 29 grudnia 2016 r. w sprawie planowania i rozliczania działalności bieżącej w Wojskowym Instytucie Medycyny Lotniczej.

Dyrektor WIML

DYREKTOR
WOJSKOWEGO INSTYTUTU MEDYCYNY LOTNICZEJ
płk dr n. med. Alicja TROCHIMIUK

.....

płk dr n. med. Alicja TROCHIMIUK

WOJSKOWY INSTYTUT MEDYCYNY LOTNICZEJ

PION ADMINISTRACYJNY

Egz. Poj.

AKCEPTUJĘ

……

REJESTR RYZYKA
DO PLANU DZIAŁALNOŚCI WIML NA 20…… ROK

WARSZAWA

20….

Wojskowy Instytut Medycyny Lotniczej

(Nazwa działu / pionu / jednostki / komórki organizacyjnej)

Cel działu/pionu/jednostki/komórki organizacyjnej*	Uzyskanie wysokiego wskaźnika poziomu przygotowania zawodowego personelu medycznego (lekarskiego, pielęgniarskiego, ratowników medycznych)
Cel z planu sporządzanego przez bezpośredniego przełożonego	Cel Nr C.5.1. Podnoszenie kwalifikacji personelu medycznego podmiotów leczniczych dla których MON jest organem tworzącym (SPZOZ i IB).
Zadanie	Doskonalenie zawodowe personelu medycznego (lekarskiego, pielęgniarskiego, ratowników medycznych)
Zadanie jednostki/komórki organizacyjnej	Organizacja i realizacja doskonalenia zawodowego personelu medycznego (lekarskiego, pielęgniarskiego, ratowników medycznych)

Identyfikacja ryzyka			**Analiza (ocena) ryzyka**				**Reakcja na ryzyko**	
Lp.	Właściciel ryzyka	Zidentyfikowane ryzyko	Prawdopodobieństwo wystąpienia	Skutek wystąpienia	Wynik (ryzyko = prawdopodobieństwo x skutek)	Poziom ryzyka	Sposób reakcji na ryzyko	Działania planowane stosownie do sposobu reakcji na ryzyko
Kategoria podstawowa** Obszar : Ośrodek Kliniczny								
1	Kierownik Ośrodka Klinicznego	nieprawidłowo rozplanowany harmonogram szkoleń	3	4	12	wysoki	działanie	- weryfikacja planu szkolenia z udziałem kierowników podległych komórek
2	Kierownik Ośrodka Klinicznego	zdarzenia wykluczające pracownika ze szkolenia	3	4	12	wysoki	działanie	zaplanowanie rezerwowych uczestników szkolenia
Kategoria zarządcza** Obszar : Pion Administracyjny								
1	Szef Pionu Administracyjnego	niewłaściwie przygotowana SIWZ	1	4	4	niski	działanie	standardowa weryfikacja dokumentów
Kategoria wspierająca** Obszar : Pion Głównego Księgowego								
	Główny Księgowy	opóźnione płatności powodujące zwiększenie kosztu	2	2	4	niski	działanie	standardowa weryfikacja zobowiązań płatniczych

Wojskowy Instytut Medycyny Lotniczej
(Nazwa działu / pionu / jednostki / komórki organizacyjnej)

Cel działu/pionu/jednostki/komórki organizacyjnej*			Uzyskanie wysokiego …….					
Cel z planu sporządzanego przez bezpośredniego przełożonego			Cel Nr C.5.1. Podnoszenie kwalifikacji ……					
Zadanie			Zapewnienie funkcjonowania i nadzór nad …….					
Zadanie jednostki/komórki organizacyjnej			Planowanie, realizacja i prawidłowe rozliczenie ……..					
Identyfikacja ryzyka			**Analiza (ocena) ryzyka**				**Reakcja na ryzyko**	
Lp.	Właściciel ryzyka	Zidentyfikowane ryzyko	Prawdopodobieństwo wystąpienia	Skutek wystąpienia	Wynik (ryzyko = prawdopodobieństwo x skutek)	Poziom ryzyka	Sposób reakcji na ryzyko	Działania planowane stosownie do sposobu reakcji na ryzyko
Kategoria podstawowa** Obszar : Ośrodek Kliniczny								
1	Kierownik Ośrodka Klinicznego	nieprawidłowo rozplanowane potrzeby …	3	4	12	wysoki	działanie	- weryfikacja planu zakupów …
2	Kierownik ….	nieprawidłowe wnioski …	3	4	12	wysoki	działanie	zaplanowanie …….
Kategoria zarządcza** Obszar : Zastępca Dyrektora ds. Naukowych								
1	Szef Pionu	niewłaściwie rozpoznanie …	3	4	12	wysoki	działanie	kwartalna ocena realizowanych ….
Kategoria wspierająca** Obszar : Pion Głównego Księgowego								
1	Główny Księgowy	nieprawidłowy kosztorysy	2	2	4	niski	działanie	weryfikacja kosztorysów …

Opracował:

Szef Pionu Administracyjnego

…….

Wykonał: …….
tel. 261 852 …….
WIML_Rejestr_Ryzyka_na_20XX_'220316_wyc_do_druku